DISEÑO DE UN MODELO DE NEGOCIO PARA OFRECER SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN A PYMES DEL SECTOR SALUD EN BOGOTÁ

ALEXANDRA RAMÍREZ CASTRO

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN ADMINISTRACIÓN MBA

BOGOTÁ

2021

DISEÑO DE UN MODELO DE NEGOCIO PARA OFRECER SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN A PYMES DEL SECTOR SALUD EN BOGOTÁ

ALEXANDRA RAMÍREZ CASTRO

Trabajo de grado presentado como requisito para optar al título de magister en

Administración de Empresas

Luz María Rivas Montoya, PhD.

Directora

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN ADMINISTRACIÓN MBA

BOGOTÁ

2021

Resumen

La seguridad de la información busca su protección de posibles daños por revelación y uso no autorizado; dado que ha cobrado fuerza con el incremento en el uso de información digital, las tecnologías de la información (TICs), la interconexión para la comunicación, negociación y prestación de servicios; también en los eventos disruptivos, como es el caso de la actual pandemia. En el sector de servicios de salud lo anterior toma relevancia por el uso de información médica, considerada confidencial y sensible, y cuya revelación no autorizada puede afectar a las personas y su integridad física y psicológica.

Si bien existe regulación que busca proteger el derecho básico de las personas a la intimidad y atender a su protección por estigmas sociales asociados a factores de enfermedad, en el sector salud aún no se brinda la relevancia requerida para proteger estos datos, que a la vista de criminales resultan llamativos por su valor en el mercado ilegal. Además, las condiciones económicas y de desconocimiento agravan esta situación en las pequeñas y medianas empresas (Pymes), dado que presentan retos en el momento de implementar controles para proteger la información de usuarios y pacientes.

Este trabajo pretender identificar los elementos que pueden influir en la implementación de la seguridad de la información en las Pymes del sector salud en la ciudad de Bogotá y propone un modelo de negocio basado en el Canvas de Osterwalder & Pigneur (2011). Para ello se realiza una revisión de literatura entre los años 2000 y 2020 en relación con el tema.

Palabras clave: modelo de negocio, Pymes de salud, seguridad de la información.

Abstract

Information security seeks to protect this from possible hurts for unauthorized disclosure and use. It has gained strength with the increase in to use of digital information, information technologies (TICs), the interconnection for communication, negotiation, and provision of services, as well as disruptive events such as the current pandemic. In the healthcare sector, the above takes relevance for the use of medical information that is considered confidential and sensitive, and whose unauthorized disclosure may affect people and their physical and psychological integrity.

Although there are regulations that seek to protect the people's basic right to privacy and attend to their protection due to social stigmas associated with disease factors; in the healthcare sector, the relevance required to protect these data isn't yet provided, which in the eyes of criminals are striking for their value in the black market. Furthermore, the economic conditions and ack of knowledge aggravate this situation in SMEs since they present challenges when implementing controls to protect users and patient information.

This work aims to identify the elements that can be included in the implementation of information security in SMEs in the healthcare sector in Bogotá city and propose a business model based on the Osterwalder & Pigneur Canvas (2011). For this, a literature review is carried out between the years 2000 and 2020 in relation to the subject.

Keywords: business model, healthcare SMEs, information security.

Contenido

Lista de Tablas

Lista de Figuras

Introducción

La seguridad de la información se ha interesado por proteger la confidencialidad (evitar el conocimiento por personas no autorizadas), la integridad (prevenir modificaciones no autorizadas) y la disponibilidad (que se encuentre al alcance de los usuarios autorizados en el momento indicado) de la información a lo largo de la historia. La industria de servicios de salud no es la excepción, especialmente, desde que se ha dado importancia al concepto de privacidad como uno de los principios de la seguridad, que busca proteger la información del individuo y emplear controles para asegurar que esta información no sea divulgada o accedida de forma no autorizada (Harris & Maymi, 2016), particularmente cuando se trata de información médica, considerando que las instituciones de salud tienen desafíos en esta área porque las fallas en la protección de esta información pueden dañar la imagen de los individuos cuando se trata de enfermedades crónicas; con esto, se puede afectar la confianza de los clientes en los servicios de salud (Kissi, Baozhen, Clemency, & Amoah-Anomah, 2018) causando pérdidas económicas y daño en la reputación de los proveedores de este tipo de servicios (Fatima & Colomo-Palacios, 2018) así como también puede impactar el valor de mercado de estas organizaciones (Von Roessing, 2010).

Algunas de las amenazas de seguridad de la información más comunes a las que se exponen los servicios de salud, y con ello la información de sus clientes, son el *ransomware*, el *phishing* y actualmente los portales web maliciosos, creados para divulgar información falsa sobre el COVID-19. Este tipo de amenazas han estado presentes por mucho tiempo; no obstante, durante la pandemia se ha incrementado su difusión, incluso a través del uso de *malware* o métodos nunca vistos en ciberataques, pasando del 20% antes de la pandemia a una proporción del 35% durante pandemia, de acuerdo con lo indicado por un análisis de la firma Deloitte (Nabe, s.f.). El

ransomware es una clase de *malware*[1] cuyo objetivo es extorsionar a la víctima a partir de impedir el uso del dispositivo hasta que no se haya pagado un rescate (Kaspersky, s.f.), por su parte, el *phishing* es una forma de robo de identidad en el que un estafador usando un correo electrónico de apariencia autentica, suplanta a una entidad buscando engañar a los destinatarios para que proporcionen información confidencial, a través de sitios web falsos a los que son dirigidos una vez dan clic en un link que es incluido en el correo (Phishing, s.f.). En el caso de los portales web maliciosos, la Interpol ha indicado que se han registrados dominios en Internet que contienen términos como “coronavirus”, “corona-virus”, “covid19” y “covid-19”. Mientras algunos son sitios web legítimos, los criminales están creando miles de sitios para realizar campañas de *spam*[2], *phishing* y difundir *malware*.

Más allá de un aspecto de cumplimiento normativo, las instituciones prestadoras de servicios de salud deben actuar con responsabilidad social empresarial frente al adecuado manejo de los datos entregados por sus clientes. Es por esto por lo que su operación, independiente del tamaño de la organización, debe considerar medidas administrativas, técnicas y físicas para proteger la información médica.

La implementación de seguridad debería estar estrechamente asociada con la adopción de tecnologías de la información. Sin embargo, las Pymes no implementan seguridad porque su preocupación está en poder operar con recursos limitados. En este sentido, aunque adopten tecnologías de la información por necesidades de operación, no significa que la implementación de estas tecnologías incluya su aseguramiento y con ello el aseguramiento de la información de la empresa y los clientes. En el caso de las empresas prestadoras de servicios de salud se considera

[1] Software o programa malicioso y dañino para los sistemas (Malwarebytes, s.f.).

[2] Cualquier tipo de comunicación digital no deseada y no solicitada, a menudo por correo electrónico que se envía de forma masiva (Malwarebytes, s.f.)

información crítica y que requiere protección: los registros médicos electrónicos, las historias clínicas y los sistemas de gestión de salud a través de los cuales se administra esta información.

En algunos casos la seguridad de la información no es un problema tecnológico, es un problema económico y la forma de mejorar la seguridad de la información es solucionar los problemas económicos (Schneier, 2007). En este sentido, las propuestas de valor en seguridad de la información destinadas a las Pymes deben considerar la optimización de recursos y actividades, de forma tal que sean costo efectivas a sus intereses y modelos propios de negocio.

El propósito de este trabajo es diseñar un modelo de negocio que permita ofrecer una propuesta de valor de servicios de seguridad de la información a Pymes del sector salud en Bogotá. Para ello, primero se realiza una revisión literaria sobre modelos de negocio y requerimientos de seguridad de la información para empresas del sector salud, detallando aquellas clasificadas como Pyme en Colombia (Ver Tabla 4 Clasificación empresarial en Colombia). A partir de lo anterior se identifican los elementos necesarios que debe tener la propuesta de valor de servicios de seguridad de la información para que se adapte de forma costo eficiente a estas Pymes. Después se identifican las actividades, recursos y asociaciones claves que permitan entregar la propuesta de valor con una ventaja competitiva. Así mismo, se plantea el modelo de ingresos y la estructura de costos requerida para plantear un modelo de negocio de bajo costo.

Con lo anterior, se busca definir una estrategia competitiva para una empresa de servicios que permita crear un posicionamiento de valor único y exclusivo (Porter, 1996) en servicios de seguridad de la información ofrecidos a las Pymes del sector salud desde el desarrollo de actividades diferentes o con mejoras a las realizadas por la competencia. La estrategia se materializa en una propuesta de valor relevante y sostenible, considerando una combinación de

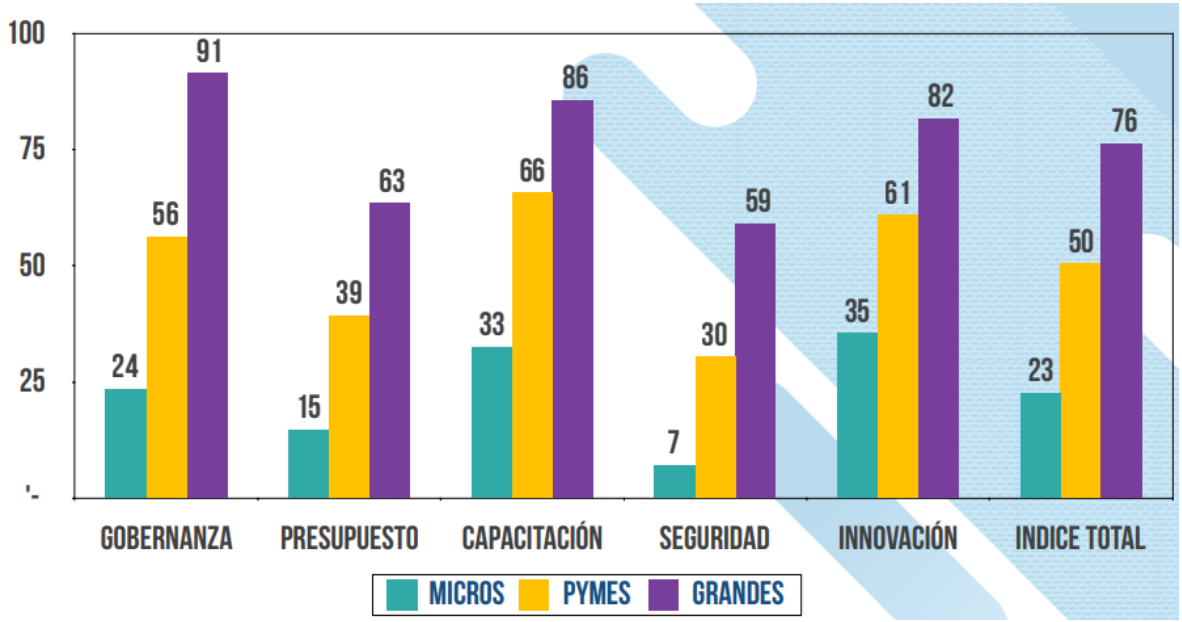
elementos que permitan su construcción bajo una ruta híbrida o de diferenciación acorde con el reloj estratégico de Bowman (Johnson, Scholes, & Whittington, 2006), manteniendo el equilibrio entre el precio que representa la estrategia y su valor percibido o inclusive con un valor percibido mayor al de la competencia, que permita determinar una propuesta de valor relevante y sostenible para los segmentos de clientes específicos. Se considera cómo se entrega esa propuesta, cuáles son las capacidades estratégicas para llevarla y determinar cuál puede ser la ventaja competitiva que se puede establecer. La estrategia se representará a través de un modelo de negocio que permita identificar en qué negocio está la empresa de servicios y describir las bases sobre las cuales se crea, entrega y captura valor (Osterwalder & Pigneur, 2011) en los servicios de seguridad de la información para el sector salud.

Planteamiento del Problema

La evolución de las tecnologías de la información en los diferentes ámbitos ha llevado a que las industrias identifiquen la necesidad de aplicar y adoptar tecnologías como parte de sus actividades y operaciones diarias, con fines de prestar productos y servicios que se mantengan a la vanguardia en la industria (Semana, 2007). De esta forma las organizaciones han visto la oportunidad de adoptar tecnologías para las actividades implicadas en la producción, comercialización, logística y mercadeo requeridos.

En Colombia, la adopción y uso de tecnologías en las empresas va a pasos gigantes. Esto se encuentra en estudios como El Observatorio de la economía digital de Colombia de 2017 (Katz, 2017) en el cual se identificó que la adopción de tecnologías digitales maduras (tales como Ciberseguridad, Computación en la nube, Internet de las Cosas, Robótica, *Big Data*, Inteligencia Artificial, entre otras) ha crecido y la brecha entre empresas grandes, medianas, pequeñas y micro respecto a la adopción de estas tecnologías ha disminuido. El informe indica que para el año 2015 el índice de adopción de tecnologías maduras era del 70,7% en empresas grandes, en las Pymes del 35% y en las microempresas del 21%; mientras al año 2017 esas cifras cambiaron en 76% para empresas grandes, 60% para Pymes y 52% para microempresas. Lo anterior presenta un incremento del 25% en Pymes; aunque este incremento no se da en todos los sectores industriales (por ejemplo, sectores de manufactura, comercio y construcción se encuentran rezagados). En cuanto a la gestión de tecnologías que incluye la gestión de seguridad, es baja en micros, pequeñas y medianas empresas respecto a la gestión de las grandes empresas como se ilustra en la Figura 1. De igual forma, entre los componentes evaluados en la gestión de tecnologías, se identifica que seguridad es el más bajo, incluso en las grandes empresas (Katz, 2017).

Figura 1. Índice de Gestión de Tecnologías Maduras en Colombia 2017.



Fuente: El Observatorio de la economía digital en Colombia (p. 22), (Katz, 2017, p. 22).

Nota: El gráfico representa los niveles de gestión de tecnologías maduras que considera gobernanza, presupuesto, capacitación, innovación y gestión de seguridad. Para esta última los niveles de gestión en micro y pequeñas empresas es menor, respecto a las grandes empresas.

Parte de los desafíos que planteó el estudio a nivel nacional fueron (Katz, 2017) que solo el 23% de las microempresas del estudio, tienen áreas o personal a cargo de gestionar la tecnología de la empresa y en una menor medida (17%) cuentan con presupuesto para tecnología. De otra parte, solo el 36% de las Pymes y el 8% de las microempresas cuentan con un área o personal a cargo de la seguridad informática.

Desde el inicio de la pandemia causada por el COVID-19, la aceleración en la transformación digital para las empresas ha mostrado un aumento significativo; con la adopción de las tecnologías de la información como elemento requerido para la reactivación empresarial y las nuevas estrategias de negocio. En un estudio de la situación de las Pymes colombianas ante el

COVID-19 realizado por la agencia mundial de comunicación Edelman, por encargo de Microsoft Colombia (News Center Microsoft Latinoamérica, 2021) se identificó que 9 de cada 10 Pymes consideran que la adopción de nuevas tecnologías, el software de videollamadas, los equipos de cómputo portátiles y el almacenamiento en la nube han sido de las principales tecnologías adoptadas durante este periodo. El 66% de las Pymes manifestó sentirse preparada para la adopción de nuevas tecnologías, sin embargo, su conocimiento para aprovechar estas se encuentra en desarrollo y consolidación. Por ejemplo, el 43% de las Pymes indicó tener conocimiento sobre *Big Data & Analytics*, el 40% en inteligencia artificial y el 54% en visualización de datos.

Dada la exigencia sobre el distanciamiento social, pero en igual medida la necesidad de las empresas por conectarse con sus clientes; la incursión de herramientas de *marketing* digital aumentó. El 65% de las empresas encuestadas consideró que fue uno de los aspectos que cambió de forma más significativa, especialmente con el mayor uso de redes sociales y sitos *webs* corporativos. Sumado al aumento del *marketing* digital, de acuerdo con un informe de la Cámara Colombiana de Comercio Electrónico y el Ministerio de Tecnologías de la Información y las Comunicaciones (Picón, 2020), el comercio electrónico se incrementó en un 73% entre abril y mayo de 2020 como medio de pago no presencial, justo en el inicio de los periodos de cuarentenas en Colombia.

En estos aspectos las empresas de salud no fueron una excepción. El incremento de la comunicación a través de redes sociales, mensajería electrónica, *chatbots* y videollamadas con usuarios y pacientes presentó incremento para brindar información sobre lineamientos y directrices ante el COVID-19, así como ofrecer agendamiento de citas, servicios de consultas virtuales y charlas en vivo con especialistas para divulgación de temas relacionados con la salud; lo cual se identificó como un efecto positivo de acuerdo con un análisis realizado por la revista *Semana*:

> *Desde visitas de atención primaria hasta de emergencia, la atención médica virtual puede ayudar a mejorar la experiencia del paciente, reducir los costos para los hospitales y los pacientes, así como reducir las estadías hospitalarias innecesarias. Y esas ventajas se notaron en plena pandemia. En Colombia, por ejemplo, según el Ministerio de Salud, durante el confinamiento más de 30 millones de colombianos tuvieron servicios de teleconsulta, y el país multiplicó hasta en 20 su capacidad en telesalud y teleorientación en los últimos seis meses* (Semana, 2020).

Se identificaron casos específicos de instituciones médicas como *Mederi* (agrupación de caja de compensación Compensar, la Orden Hospitalaria San Juan de Dios y la Universidad del Rosario), *Keralty* y las EPS Sanitas y Colsanitas, que a través de transformación tecnológica acelerada digitalizaron especialidades médicas con lo cual aumentaron su capacidad de atención por teleconsultas, así como también aumentaron el cubrimiento a nivel país. Además de estos cambios desde las empresas prestadoras de salud, terceros en la cadena de valor implementaron y mejoraron herramientas complementarias a los servicios médicos, tales como farmacias en línea, *marketplaces* para el abastecimiento de insumos hospitalarios, lectura de imágenes diagnósticas con inteligencia artificial, entre otros (Semana, 2020). Con lo anterior, en los últimos meses se ha visto más innovación en el sector salud, que, en años, de acuerdo con lo indicado por Alex Coqueiro, director de tecnología para el sector público de *Amazon Web Services* para Latinoamérica, el Caribe y Canadá.

Entre los datos relevantes del estudio de Edelman y Microsoft, un 58% de las Pymes encuestadas (cerca de 197 empresas del país con hasta 250 empleados) manifestaron preocupación por la ciberseguridad en el nuevo entorno digital, en el estudio también se detectó que las empresas de mayor tamaño robustecieron los sistemas de ciberseguridad. En el caso del sector de la salud, los avances en telemedicina abren apuestas por la implementación de tecnologías como

inteligencia artificial y *machine learning*, analítica de datos y *blockchain*; que junto con el manejo de información privada y sensible, se considera será clave que las tecnologías a implementar garanticen la seguridad de los pacientes y sus datos, además considerando las pautas iniciales sobre historia clínica digital, ley 2015 de 2020 (Ministerio de Salud, 2020), con lo cual se abre una puerta hacia la ciberseguridad, indica Alonso Verdugo, *chief medical officer* de Microsoft para Latinoamérica.

Sin embargo, a pesar de los requerimientos de los mercados, la coyuntura por pandemia y el papel relevante que ha tomado la tecnología en los negocios, haciendo más digitales a las empresas y especialmente a las Pymes (News Center Microsoft Latinoamérica, 2021), la acogida de medidas de protección no se ha dado a la misma velocidad de la adopción de tecnologías; en parte por los requisitos de inversión que implica implementar estas medidas y adicional porque las empresas no reconocen la necesidad de proteger las actividades y procesos del negocio en toda la cadena de valor, así como la información y los datos que se manejan a través de esta, junto con el desarrollo de conocimientos que no solo permitan la implementación de tecnologías sino hacer esta en condiciones de seguridad, generando confianza en los clientes. A la par de la evolución e inclusión de las tecnologías en las cadenas de producción y distribución de productos y servicios, las amenazas que pueden afectar estos recursos han evolucionado y es necesario establecer medidas técnicas y humanas para su protección. En el caso particular del sector salud, ejemplos como la suplantación a entidades a través de mensajería electrónica enviada a usuarios y las fallas en seguridad para el acceso a portales web con fines de agendar citas u obtener resultados de exámenes clínicos, son amenazas latentes.

Lo anterior representa un desafío para las empresas en cuanto a privacidad, protección de datos e información, más aún para las Pymes y microempresas; agregando que aunque se ha

avanzado en la adopción de tecnologías y la disminución de la brecha tecnológica, su uso efectivo no se encuentra a la par, debido al analfabetismo digital y desaprovechamiento tecnológico (Carvajal, 2021).

En entrevistas realizadas a profesionales e investigadores reconocidos del ámbito de la seguridad de la información en diferentes industrias, se presentan en la Tabla 1 puntos de vista respecto a la relación entre inversiones en seguridad, el incremento en brechas y la inclusión de tecnologías en las empresas.

Tabla 1. Consideraciones sobre inversión en seguridad y reducción de riesgos

Profesional (Empresa)	**Consideración entre la relación inversión seguridad - reducción riesgos**	**Qué determina el profesional como importante**
David Kennedy (*TrustedSec*)	No hay relación directa	Tener claridad en qué se quiere proteger, qué puede representar un factor de riesgo y amenaza para determinar los recursos a destinar a su protección. Invertir en el capital humano (ingeniería) que cuente con las capacidades de soportar la tecnología en la que se invierte, más que considerar la misma tecnología.
Ron Gula (*Tenable Network Security*)	Se incrementa inversión pero se incrementan los riesgos	Las empresas trabajan fuertemente en seguridad porque los adversarios gastan más recursos en obtener sus objetivos.
Dug Song (Cisco)	La inversión puede ayudar a reducir riesgos, solo si la tecnología se sabe usar.	Las brechas de seguridad están aumentando porque las empresas están pasando por una transformación digital. La implementación de seguridad debe considerar lo que actualmente la gente quiere adoptar y no considerar comportamientos no naturales.

Profesional (Empresa)	Consideración entre la relación inversión seguridad - reducción riesgos	Qué determina el profesional como importante
Robert Lee Drago (s Inc.)	No hay relación precisa	La inversión en seguridad es un tema de percepción que implica revisión de varios años.

Fuente: Elaboración propia a partir de (Carey & Jin, 2019).

Las grandes empresas por su tamaño, número y valor de activos, ventas, ingresos, cantidad de trabajadores, cantidad de clientes, número de transacciones u operaciones y requerimientos legales y regulatorios, han adoptado medidas en seguridad informática, seguridad de la información y gestión de riesgos que les permiten tener algunos niveles de protección de la información propia y de sus clientes. La compañía de seguridad informática *Eset,* en su reporte de seguridad para Latinoamérica en 2018 (Eset, 2018) consultó con 2.500 empresas catalogadas entre pequeñas, medianas, grandes y *Enterprise* el porcentaje de empresas con incidentes de *malware,* encontrando que a menor tamaño de la empresa, consideran no haber tenido incidentes de seguridad, sin embargo, esto puede corresponder a falta de preparación para identificarlos, dado que no cuentan con los mecanismos, conocimientos, personal y herramientas para esto.

Algunos de los aspectos por los cuales las Pymes no consideran contar con medidas de seguridad se presentan en la Tabla 2.

Tabla 2. Posibles aspectos por los cuales las Pymes no implementan seguridad

Aspecto	Descripción	Fuentes
Manejo de prioridades y dedicación de personal	Implementar, operar y mantener la seguridad no se considera una prioridad. En muchos casos no existe personal capacitado, dedicado o interesado en esto, posiblemente por aspectos presupuestales.	(Eset, 2018), (Vector ITC, 2018), (Sothis, s.f.), (AT&T, s.f.)

Aspecto	Descripción	Fuentes
Costos	Aunque se considera relevante, no se cuenta con los recursos financieros para la implementación o lo consideran costoso, desconociendo que puede haber diferentes opciones.	(Osores, 2021), (Red Seguridad, 2020), (Ascentor, s.f.)
Riesgos de seguridad y su exposición para Pymes	Desconocimiento de los riesgos a los cuales están expuestos sus recursos (información, infraestructura tecnológica, know-how, entre otros), así como creen que estos no son de interés para atacantes.	(Semana, 2013), (Vector ITC, 2018), (Kaspersky, 2017), (Red Seguridad, 2020), (Sothis, s.f.), (Ascentor, s.f.), (Yaping, 2018)
Desconocimiento de medidas de protección	Tales como: contar con *backups* para recuperar la información, dispositivos y configuraciones de seguridad para proteger la red, uso de aplicaciones licenciadas para disminuir riesgo de infección por *malware* y capacitación al personal.	(Kaspersky, 2017), (Sothis, s.f.), (Lipman, 2020)
Regulación en seguridad aplicable	Se desconoce o resta importancia a los aspectos regulatorios relacionados con seguridad. Por ejemplo, protección de datos personales, información financiera y *copyright*.	Identificado a partir de la experiencia del autor de este texto en actividades de consultoría
Mitos como: el antivirus es toda la seguridad que se necesita	Se considera que con esta implementación se está “a salvo” de amenazas. Inclusive se llega a considerar la adquisición de soluciones antivirus gratuitas, que no cuentan con las funcionalidades necesarias para proteger a la empresa.	(Lipman, 2020), (Jones, 2002)

Fuente: Elaboración propia a partir de las fuentes referidas.

Incluso, aunque las grandes empresas cuentan con esquemas y áreas encargadas de seguridad de la información, en varios casos estos no son robustos porque no consideraron implementar controles de seguridad desde que iniciaron sus actividades como micro, pequeñas o medianas empresas. Contar con estos esquemas y hacerlos crecer a la par del negocio, ayudaría a mitigar la exposición a amenazas en mayor medida.

Lo anterior no significa que 1) se busque que las empresas estén cien por ciento seguras, dado que no es posible debido a la misma evolución de las amenazas, o 2) que se considere que la situación no puede mejorar, porque los modelos de seguridad pueden ser cada vez más robustos. La finalidad es lograr que las Pymes tengan esquemas de seguridad de la información para proteger su negocio a la par de la evolución del mercado.

A nivel gubernamental, el Ministerio de Tecnologías de la Información y la Comunicación publicó la Guía para la implementación de seguridad de la información en una MiPyme (MinTIC, 2016) como parte del marco de guías del modelo de seguridad y privacidad de la información, a través de la cual se dio un panorama de seguridad para las empresas y se buscó brindar herramientas para implementar medidas de seguridad. De otra parte, el Centro Cibernético Policial para el mismo año publicó un Boletín de análisis en ciberseguridad Pyme (Policia Nacional, 2016) como una guía para evitar la suplantación de clientes y proveedores. Sin embargo, hay dos temas, posteriores a la publicación de estas guías en el año 2016: 1) no ha sido publicado nueva información para las Pymes considerando que los mecanismos de ataque siguen evolucionando, y 2) no se consideran las características propias de cada sector industrial, acorde con su tamaño y requerimientos de operación, con lo cual pueden diferir los requerimientos de seguridad y las posibilidades para implementar mecanismos de protección por parte de estas.

A nivel de empresa privada, en Colombia hay presencia de empresas que ofrecen productos y soluciones de seguridad para Pymes, sin embargo, estas se limitan al hardware y al software puestos a disposición de las empresas, como es el caso de las soluciones de seguridad para pequeños negocios ofrecidas por la empresa Kaspersky (Kaspersky, 2019). Estas pueden cubrir el aspecto de costos mencionado, dado que los valores de estos productos están al alcance de las Pymes, pero no dan cubrimiento a todos los aspectos requeridos, tales como conocimiento de

riesgos para identificar qué se debe proteger y cómo, y personal dedicado a implementar, operar y mantener esos productos; por lo cual se puede crear una falsa sensación de seguridad.

Lo anterior permite plantear la utilidad en el diseño de una propuesta de valor enfocada en servicios de seguridad de la información, que permita cubrir, bajo un esquema de componentes o piezas, los requisitos de seguridad de las Pymes, considerando el contexto mencionado. Estos componentes contemplan hardware, software y personal calificado para brindar asesoría y servicios gestionados de seguridad.

Entonces se consideró inicialmente como problemática encontrar bajo las condiciones del ecosistema de negocios que implican factores de mercado, necesidades empresariales, recursos humanos y económicos finitos, mitos en relación con la protección y otros; ¿Qué debe tener una propuesta de servicios de seguridad de la información que se adapte a las limitaciones y necesidades que tienen las Pymes colombianas?

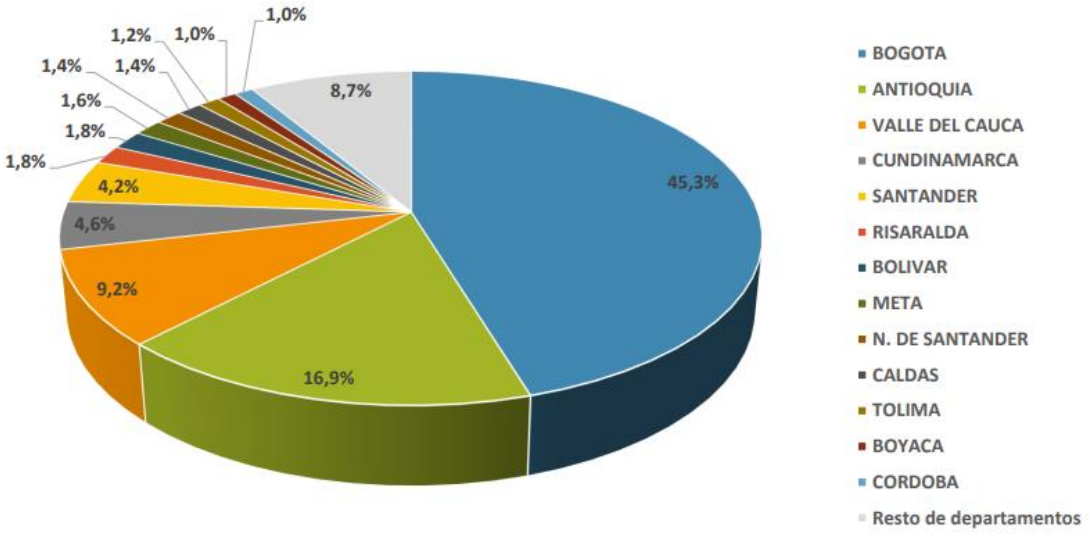
A partir de este primer acercamiento se realizó un análisis de los sectores económicos en los que se ubican las Pymes en Colombia (manufacturero, servicios y comercio) encontrando diferentes agrupaciones dentro de estos sectores que pueden tener necesidades específicas de seguridad, de acuerdo con su operación. Por ejemplo, en Bogotá se encuentran los clústeres de salud, servicios financieros, construcción, energía eléctrica, industrias creativas, entre otros, (Cámara de Comercio de Bogotá, s.f.). En Medellín se encuentran los clústeres de energía sostenible, hábitat sostenible, turismo de negocios, Medellín *health city*, entre otros, (Cámara de Comercio de Medellín, 2020); y de forma similar se pueden encontrar diferentes agrupaciones a nivel país. Sin embargo, considerando las características en la operación de cada sector y las necesidades específicas en relación con seguridad de la información, así como los elementos

regulatorios que pueden obligar a un sector u otro a cumplir con requisitos de seguridad, la problemática se acota a una propuesta de servicios de seguridad de la información para Pymes del sector salud.

Este sector fue seleccionado por qué se identificó que es uno de los sectores que maneja información de mayor sensibilidad, al tratarse de datos médicos y de salud de los ciudadanos, esta información debe ser protegida al ser estos considerados datos sensibles bajo los parámetros de la legislación colombiana. Los datos e información médica están amparados por la ley estatutaria 1751 de 2015 (Ministerio de salud, 2015), la ley 1581 de 2012 sobre la protección de datos personales (Secretaría Senado, 2019), y la ley 2015 de 2020 por la cual se crea la historia clínica electrónica (Ministerio de salud, 2020), entre otras. Además, por análisis realizados frente a la seguridad de información personal, el sector salud es uno de los destacados frente a la falta de preocupación e interés para implementar medidas de seguridad (Caracol Radio, 2017). Por lo anterior, es una obligación y debería ser un punto de interés para las empresas del sector salud implementar mecanismos de protección; con lo cual la propuesta de valor y el modelo de negocio de servicios de seguridad de la información bajo el cual se plantea puede resultar de mayor interés y beneficio.

De otra parte, el alcance geográfico se limita a las Pymes ubicadas en Bogotá, por su representación porcentual respecto a las Pymes del país. En el año 2018, en Colombia el porcentaje de pymes era del 6.74%, correspondiente a 109.220 pequeñas y medianas empresas sobre la totalidad de empresas colombianas, que para el mismo año rondaba la cifra de 1.620.342 (Economía Aplicada, 2019). A junio de 2019, la cantidad de Pymes en Colombia se encontraba en 108.223, de las cuales el 45.3% están ubicadas en la ciudad de Bogotá (Cámara Comercio Medellín, 2019). La distribución de Pymes en Colombia se presenta en la Figura 2.

Figura 2. Pymes en Colombia y su distribución por departamentos.



Fuente: (Cámara de Comercio de Medellín, 2019, p. 4)

El alcance excluye las microempresas, dado que por su tamaño, ingresos y complejidad en operación pueden identificar limitaciones en contratar servicios de seguridad de la información a través del modelo de negocio a desarrollar. En este sentido la pregunta de investigación se acota como: ¿Qué debe tener una propuesta de servicios de seguridad de la información que se adapte a las limitaciones y necesidades que tienen las Pymes colombianas del sector salud? y sobre esta se realizó el desarrollo de este trabajo.

Justificación

La información de salud personal es relevante para diferentes grupos de interés, puesto que la necesitan y utilizan como fuente de trabajo, investigación y beneficio. En este sentido, cada uno tiene una percepción de su valor en relación con su utilidad, pero sin importar el grado de valor en el cual sea percibida, debe considerarse su protección. En la Tabla 3 se presentan diferentes grupos de interés de los datos de salud y las razones por las cuales pueden requerirse.

Tabla 3. Interés por los datos de salud acorde con grupos de interés

Grupos de interés	**Beneficio y uso de los datos**
Proveedores de servicios de salud	Registros de pacientes para toma de decisiones diagnósticas y terapéuticas
Compañías de seguros	Datos de salud personal para facilitar predicción de riesgos para la salud de asegurados y no asegurados, que les permita adaptar primas o renunciar a contratos
Universidades, Organizaciones de investigación y farmacéuticas	Datos de pacientes para desarrollar y probar nuevos diagnósticos y fármacos
Empresas orientadas al consumo	Información de salud personal para optimizar el *marketing* de productos
Pacientes	Los propios datos médicos para mejorar la salud cuando estos son utilizados por profesionales del ámbito, pero considerando la protección de esta información

Fuente: Adaptado de (Czeschik, 2018, p. 2).

Ahora el valor monetario que se puede atribuir a estos datos según la Organización para la Cooperación y el Desarrollo Económicos (OECD), como se citó en Czeschik (2018), puede dividirse en dos clases: 1) basada en la valoración individual y 2) basado en la valoración del mercado. Como parte de la valoración del mercado, algunas medidas son los costos de las brechas de los datos y el precio de estos datos en los mercados ilegales.

Las brechas de datos en el sector salud vienen incrementándose en costos y frecuencia. Acorde con estudios del *Instituto Ponemon* sobre privacidad y seguridad de datos en salud, se estimaron costos en las brechas para la industria que ascendían en $5.6 billones para el 2014 (Ponemon Institute, 2014), $6 billones para el 2015 (Ponemon Institute, 2015) y $6.2 billones para el 2016 (Ponemon Institute LLC, 2016). Para los años posteriores no se cuenta con los datos, sin embargo, con estas cifras se identifica cómo se ha dado el incremento en las brechas. Respecto al precio de estos datos en los mercados ilegales, la división de ciberseguridad del FBI estimaba para el 2014 que el valor de un registro de salud individual era de 50 USD (Czeschik, 2018); mientras al 2017 se estimaba en 250,15 USD (Trustwave, 2018), por encima del detalle de una tarjeta de pago, que para el mismo año se estimaba en 5,40 USD. De esta forma los registros médicos representan datos de mayor interés para los criminales, porque pueden utilizarse para suplantación de identidad con el fin de acceder a servicios médicos, realizar reclamaciones de seguros fraudulentas, obtener prescripciones médicas que pueden también ser comercializadas en el mercado negro y extorsionar a instituciones y personas por no divulgar información relacionada con enfermedades crónicas o cambios estéticos, entre otros.

Czeschik (2018), menciona:

> *[…] los expertos sugieren que el sector de la salud reemplaza al sector financiero como principal objetivo de ataques cibernéticos, no solo por el valor inherente de los datos, sino porque sus defensas en seguridad son inferiores en comparación. (p. 3).*

El último estudio de *Instituto Ponemon* en 2016, también encontró que varias organizaciones de la salud y sus asociados de negocio (proveedores y terceros en la cadena de valor como las farmacias) eran negligentes en el manejo de la información de los pacientes, tema que a la fecha de este trabajo puede continuar sucediendo y causando que sigan incrementándose

las brechas. En el año 2019, durante la Feria de Electrónica de Consumo (CES), que se considera la feria de tecnología más grande a nivel mundial, fueron presentadas soluciones tecnológicas relacionadas con diagnóstico, monitoreo y tratamiento de enfermedades y soluciones asociadas con asistencia médica remota. Ahora el problema radica en las medidas de seguridad implementadas sobre estas soluciones y dispositivos, que no necesariamente siguen las mejores prácticas respecto a la protección de la información médica con posibilidades de dejar los datos de pacientes expuestos en línea (Periódico El Sol, 2019). La actual situación relacionada el COVID-19, durante la cual se han fortalecido los esquemas de asistencia médica remota, muestran los riesgos a los cuales se exponen las empresas en este sector por el tipo de información que manejan. La sustracción de datos a partir de ataques de *phishing* y el uso de portales web maliciosos creados con información relacionada con el COVID-19 se ha incrementado (Interpol, 2020), así como a nivel mundial los ataques por *ransomware* han aumentado, ubicando al sector salud en la media de empresas que ha detectado ataques de este tipo (Fortinet, 2020).

A partir del modelo de negocio presentado en este trabajo se busca ofrecer a las Pymes del sector salud en Bogotá esquemas de seguridad de la información al alcance de su negocio en términos de las necesidades específicas de operación, los requerimientos regulatorios y normativos por cumplir, las limitaciones económicas que puedan tener para invertir en la adquisición de estos servicios y el creciente uso de tecnología aplicada a salud; motivado por los aspectos mencionados respecto a brechas y valor de la información médica, considerando que aunque es un activo valioso, de acuerdo con análisis de la industria al momento no es lo suficientemente protegida en la mayoría de organizaciones de salud a nivel mundial (Czeschik, 2018).

En igual medida se busca que los esquemas de seguridad de la información operen y se mantengan a la par del crecimiento de la empresa, es decir, con el producto resultante se proyecta

incrementar el cubrimiento en seguridad de la información para las Pymes del sector Salud, sea que estas se mantengan como Pymes o crezcan y se conviertan en empresas grandes a futuro.

Como se presentó en el planteamiento del problema, la motivación de este trabajo está dada por la representación de las Pymes en el tejido empresarial colombiano y el bajo porcentaje de estas que cuentan con esquemas de seguridad de la información implementados y operando con estándares de calidad respecto a los controles de seguridad acorde a las necesidades de los negocios. De los resultados del presente trabajo se beneficiará inicialmente el sector salud, pero los siguientes pasos consideran que el modelo de negocio se pueda adaptar a diferentes sectores empresariales, identificando las necesidades propias de protección de datos e información, así como los elementos a considerar para implementar seguridad de la información.

Marco Conceptual

Como parte del marco conceptual para dar contexto al presente trabajo, se presentarán cuatro elementos: la información referente al concepto de Pyme en Colombia, las características del sector empresarial de salud como parte del subgrupo de Pymes al que da alcance este trabajo, los conceptos de seguridad de la información y cómo es percibida esta desde las Pymes y el sector salud; y lo referente a modelos de negocio, haciendo especial énfasis en el *business model Canvas*, que es el utilizado para el desarrollo del trabajo al ser menos complejo en su construcción, la presentación de sus componentes facilita la comunicación de la propuesta de valor y los elementos que permiten llevarla a los segmentos cliente.

Pymes en Colombia

Pyme es el acrónimo dado en Colombia a la pequeña y mediana empresa. A partir de diciembre de 2019, las empresas colombianas se encuentran clasificadas por rangos de ventas brutas anuales, es decir, los ingresos por actividades ordinarias que se encuentran valorados en UVTs (unidad de valor tributario), acorde con lo indicado por el Decreto 957 de 2019 (Ministerio de Comercio, Industria y Turismo, 2019). De esta forma se clasifican por sector manufacturero, servicios y comercio, como se indica en la Tabla 4.

Tabla 4. Clasificación empresarial en Colombia.

Sector	**Tipo**	**Ventas brutas anuales[3]**
Manufacturero (SM)	Micro	Hasta 23.563 UVT[4]
	Pequeña	Mayor a 23.563 UVT

[3] Ingreso por actividades ordinarias anuales
[4] UVT unidad de valor tributario. La UVT fijada para el año 2021 es de $36.308

		Hasta 204.995 UVT
	Mediana	Mayor a 204.995 UVT Hasta 1’736.565 UVT
	Grande	Mayor a 1’736.565 UVT
Servicios (SS)	Micro	Hasta 32.988 UVT
	Pequeña	Mayor a 32.988 UVT Hasta 131.951 UVT
	Mediana	Mayor a 131.951 UVT Hasta 483.034 UVT
	Grande	Mayor a 483.034 UVT
Comercio (SC)	Micro	Hasta 44.769 UVT
	Pequeña	Mayor a 44.769 UVT Hasta 431.196 UVT
	Mediana	Mayor a 431.196 UVT Hasta 2’160.692 UVT
	Grande	Mayor a 2’160.692 UVT

Fuente: Elaboración propia a partir de información del decreto 957 de junio de 2019 de (Ministerio de Comercio, 2019, p. 4).

Previa a esta nueva clasificación de las empresas colombianas, la ley 590 de 2000 (Secretaria Senado, 2000) que dicta las disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas, indicaba como factores para la clasificación de las empresas el número de trabajadores y los activos totales, como se indica en la Tabla 5. Lo cual también se considera como referencia respecto al número de trabajadores que es un punto relevante del planteamiento del problema expuesto previamente.

Tabla 5. Clasificación previa de MiPymes.

Tipo	No. Trabajadores	Activos totales
Micro	Menor de 11	Menor a 501 SMMLV
Pequeña	Entre 11 y 50	Entre 501 y menor de 5.001 SMMLV
Mediana	Entre 51 y 200	Entre 5.001 y 30.000 SMMLV

Fuente: Elaboración propia a partir de información de la ley 590 de 2000, (Secretaria Senado, 2000).

Dado que en la revisión de literatura se obtuvieron principalmente resultados de artículos de Estados Unidos y Europa, con fines de establecer una relación comparativa entre las empresas que se consideran Pymes en Colombia y aquellas de estas regiones, a continuación, en la Tabla 6 se presentan las características de clasificación de las Pymes en dichas regiones.

Tabla 6. Clasificación Pymes (SMEs) en Europa y Estados Unidos

	Unión Europea		Estados Unidos	
Tipo	**No. Trabajadores**	**Volumen de ventas[5]**	**No. Trabajadores**	**Volumen de ventas**
Micro	Menor de 10	Menor o igual a € 2M	Menor de 10	Varía según la industria
Pequeña	Entre 11 y 50	Menor o igual a € 10M	Varía según la industria	Varía según la industria
Mediana	Entre 51 y 249	Menor o igual a € 50M	Varía según la industria	Varía según la industria

Fuente: Elaboración propia a partir de información de la Unión Europea (European Commision, s.f.) y la Administración de negocio pequeños (U.S. Small Business Administration, s.f).

[5] Volumen de ventas en millones de euros

En Estados Unidos no cuentan con una clasificación estándar para identificar las Pymes. Su clasificación se da según estructura de propiedad, número de empleados, ganancias e industria. En el caso de la Unión Europea, define una clasificación clara basada en el número de empleados y el volumen de ventas. Este segundo caso, es en especial relevante dado que la clasificación de empresas por número de empleados es muy similar entre Colombia y el marco de la Unión Europea, lo cual para fines de análisis y resultados resulta relevante.

De otra parte, en el decreto 957 de 2019, el Ministerio de Comercio, Industria y Turismo en conjunto con el Departamento Administrativo Nacional de Estadística (DANE) a través de la resolución 2225 de 2019 (Ministerio de comercio, industria y turismo; Departamento administativo nacional de estadística, 2019) establecieron el anexo técnico de correspondencia de los sectores manufactura, comercio y servicios con la clasificación de las actividades económicas CIIU (clasificación industrial internacional uniforme). En este el sector salud se encuentra enmarcado en la sección de actividades de atención de la salud humana y de asistencia social, y su correspondencia está dada con el sector de servicios, como se presenta en la Tabla 7.

Tabla 7. Ubicación del Sector Salud de acuerdo con la clasificación CIIU del DANE.

Sección Q: ACTIVIDADES DE ATENCIÓN DE LA SALUD HUMANA Y DE ASISTENCIA SOCIAL			
División	**Grupo**	**Descripción**	**Sector**
86	**---**	**Actividades de atención de la salud humana**	
	861	Actividades de hospitales y clínicas, con internación	SS
	862	Actividades de práctica médica y odontológica, sin internación	SS
	869	Otras actividades de atención relacionadas con la salud humana	SS
87	**---**	**Actividades de atención residencial medicalizada**	

Sección Q: ACTIVIDADES DE ATENCIÓN DE LA SALUD HUMANA Y DE ASISTENCIA SOCIAL			
División	**Grupo**	**Descripción**	**Sector**
	871	Actividades de atención residencial medicalizada de tipo general	SS
	872	Actividades de atención residencial, para el cuidado de pacientes con retardo mental, enfermedad mental y consumo de sustancias psicoactivas	SS
	873	Actividades de atención en instituciones para el cuidado de personas mayores y/o discapacitadas	SS
	879	Otras actividades de atención en instituciones con alojamiento	SS
88	**---**	**Actividades de asistencia social sin alojamiento**	
	881	Actividades de asistencia social sin alojamiento para personas mayores y discapacitadas	SS
	889	Otras actividades de asistencia social sin alojamiento	SS

Fuente: Adaptado de la resolución 2225 de diciembre de 2019 de (Ministerio de Comercio, DANE, 2019, p. 22)

Además, entre las entidades que están en el marco de los planes adicionales de salud, como aseguradoras, se encuentran las empresas de pólizas de salud que están bajo el grupo de actividades financieras y de seguros, también con una correspondencia con el sector de servicios, como se presenta en la Tabla 8.

Tabla 8. Ubicación del sector seguros de acuerdo con la clasificación CIIU del DANE.

Sección K: ACTIVIDADES FINANCIERAS Y DE SEGUROS			
División	**Grupo**	**Descripción**	**Sector**
64	**---**	**Actividades de servicios financieros, excepto las de seguros y de pensiones**	
	641	Intermediación monetaria	SS

	642	Otros tipos de intermediación monetaria	SS
	643	Fideicomisos, fondos (incluye fondos de cesantías) y entidades financieras similares	SS
	649	Otras actividades de servicio financiero, excepto las de seguros y pensiones	SS
65	---	**Seguros (incluso el reaseguro), seguros sociales y fondos de pensiones, excepto la seguridad social**	
	651	Seguros y capitalización	SS
	652	Servicios de seguros sociales de salud y riesgos profesionales	SS
	653	Servicios de seguros sociales de pensiones	SS
66	---	**Actividades auxiliares de las actividades de servicios financieros**	
	661	Actividades auxiliares de las actividades de servicios financieros, excepto las de seguros y pensiones	SS
	662	Actividades de servicios auxiliares de los servicios de seguros y pensiones	SS
	663	Actividades de administración de fondos	SS

Fuente: Adaptado de la resolución 2225 de diciembre de 2019 de (Ministerio de Comercio, DANE, p. 18)

En el año 2018 en Colombia, el porcentaje de Pymes era del 6.74%, correspondiente a 109.220 pequeñas y medianas empresas sobre la totalidad de empresas colombianas que para el mismo año rondaba la cifra de 1.620.342 (Economía Aplicada, 2019). Tomando cifras de la Superintendencia Nacional de Salud (Supersalud, 2019) para diciembre de 2018 en el país se contaba con 116 entidades aseguradoras y 6.478 prestadores de salud para un total de 6.594 entidades de salud; de las cuales aproximadamente el 46,5%[6] estaban clasificadas como pequeñas

[6] Porcentaje calculado a partir de los reportes de la información financiera con fines de supervisión entregada por las entidades vigiladas a Supersalud, con corte a 31 de diciembre de 2018. Las entidades de las cuales se tiene información son IPS y TEP, EPS contributivo y subsidiado, EMP, SAP y Entidades de Régimen Especial y de

y medianas empresas para ese año, partiendo de la clasificación por activos totales basados en SMMLV[7]. Esto es cerca de 3.047 empresas del país. Para el 2019 (Supersalud, 2020) las entidades aseguradoras bajaron a 114 y los prestadores de servicio a 6.239 pasando el total a 6.353 entidades de salud (disminución del 3,65% respecto a 2018), de las cuales aproximadamente el 52,7%[8] serían clasificadas como Pymes. Es de notar que, aunque de un año a otro se identifica una disminución en la cantidad de entidades de salud, el porcentaje de estas que se consideran en el rango de Pymes aumentó. El principal nicho de las empresas del sector salud, se encuentra entre las IPS (Institución Prestador de Salud) y las TEP (Transporte Especial de Pacientes).

Para junio de 2019, la cantidad de Pymes en Colombia se encontraba en 108.223 empresas (Cámara Comercio Medellín, 2019). A la fecha de la investigación, no fue posible obtener información actualizada de la totalidad de empresas colombianas, así como cifras actualizadas de las empresas del sector salud. Sin embargo, la variación porcentual en el número de Pymes entre los años 2018 y 2019, con los datos presentes, aunque representa un decremento, es pequeño con un 0.91%, que representa 997 Pymes menos.

A continuación, se presentará la caracterización del sector salud en Colombia para luego establecer cómo perciben estas empresas desde el ámbito de Pymes, la apropiación de tecnologías de la información y con ello de la seguridad de la información en sus procesos de operación.

Excepción. Este porcentaje no incluye información de entidades Adaptadas, Pólizas de salud, Planes Complementarios y entidades complementarias al SGSSS (ARL y SOAT), que en total sumaban 47 entidades para la fecha corte en mención.

[7] Acrónimo de Salario Mínimo Mensual Legal Vigente

[8] Porcentaje calculado a partir de los reportes de la información financiera con fines de supervisión entregada por las entidades vigiladas a Supersalud, con corte a 31 de diciembre de 2019. Las entidades de las cuales se tiene información son IPS y TEP, EPS contributivo y subsidiado, EMP, SAP y Entidades de Régimen Especial y de Excepción.

Sector Salud en Colombia

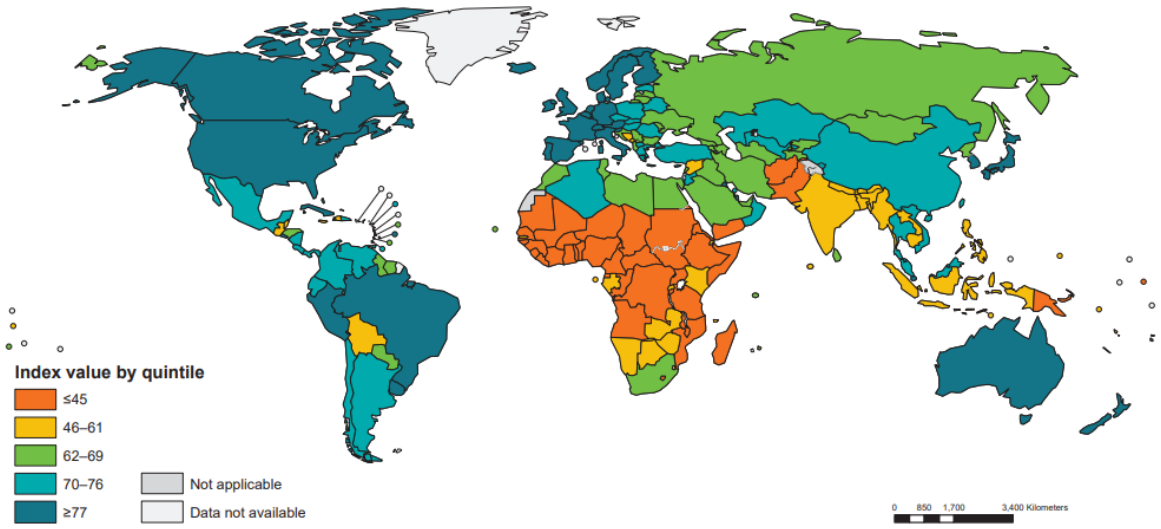
Generalidades

En la actualización de marzo de 2020 del estudio sectorial de salud (Sectorial, 2020) se indica que uno de los objetivos de desarrollo sostenible de la Organización de las Naciones Unidas (ONU) es la cobertura en salud, sin embargo, para 2015, cerca del 50% de la población en el mundo no contaba con acceso a estos servicios de acuerdo con el reporte del *World Health Statistics* de 2019 (WHO, 2019) mencionado en el mismo estudio.

El índice de cobertura universal en salud calculado por la Organización Mundial de la Salud (OMS), para el año 2015 presentaba que Colombia obtuvo un puntaje de 76/100, lo cual posicionaba bien al país en cobertura, respecto al análisis mundial, teniendo en cuenta que parte de la salud en Colombia es subsidiada, caso diferente a Estados Unidos, donde si bien el índice de cobertura es superior, el sistema de salud es privado en su totalidad. Ver Figura 3.

Independiente del esquema de acceso a salud que se maneja en el país, la propuesta de valor en desarrollo puede ser ofrecida a Pymes, en especial que se encuentren en el esquema privado (por facilidades de acceso para ofrecer los servicios respecto a los esquemas de licitación que se manejan en el sector público). Además, el nivel de cobertura se puede asociar con niveles de oferta y demanda superiores, lo cual también representa un aspecto positivo para la propuesta desarrollada.

Figura 3. Índice de cobertura de servicios de salud por país para el 2015.



Fuente: Estadísticas mundiales salud 2019, (WHO, 2019)

Para el 2019, en el ranking de los 10 mejores hospitales y clínicas de América Latina, se encontraban 4 entidades colombianas de las ciudades de Bogotá, Cali, Bucaramanga y Medellín (América economía, 2019). Las 4 entidades son de carácter privado, ver Tabla 9. Aunque la propuesta de valor originalmente se enfoca en Pymes del sector, este dato revela que las grandes empresas donde se pueden encontrar hospitales y clínicas pueden ser un mercado potencial para la oferta de servicios de seguridad.

Tabla 9. Ranking 2019 de clínicas y hospitales de Latinoamérica.

RK 2019	Hospital o Clínica	País (Ciudad)	Tipo de hospital	Índice de calidad
1	Hospital Israelita Albert Einstein	BR (São Paulo)	Privado	98.45
2	Clínica Alemana	CL (Santiago)	Privado	90.21
3	Fundación Cardioinfantil – Instituto de Cardiología	CO (Bogotá)	Universitario Privado	83.61

4	Fundación Valle del Lili	CO (Cali)	Universitario Privado	83.60
5	Hospital Italiano de Buenos Aires	AR (Buenos Aires)	Privado	80.86
6	Fundación Cardiovascular de Colombia-Hospital internacional de Colombia	CO (Bucaramanga)	Universitario Privado	77.78
7	Hospital Samaritano Higienópolis	BR (São Paulo)	Privado	77.70
8	Hospital Clínica Bíblica	CR (San José)	Privado	76.98
9	Hospital Pablo Tobón Uribe	CO (Medellín)	Universitario Privado	76.63
10	Hospital Universitario Austral	AR (Buenos Aires)	Universitario Privado	76.39

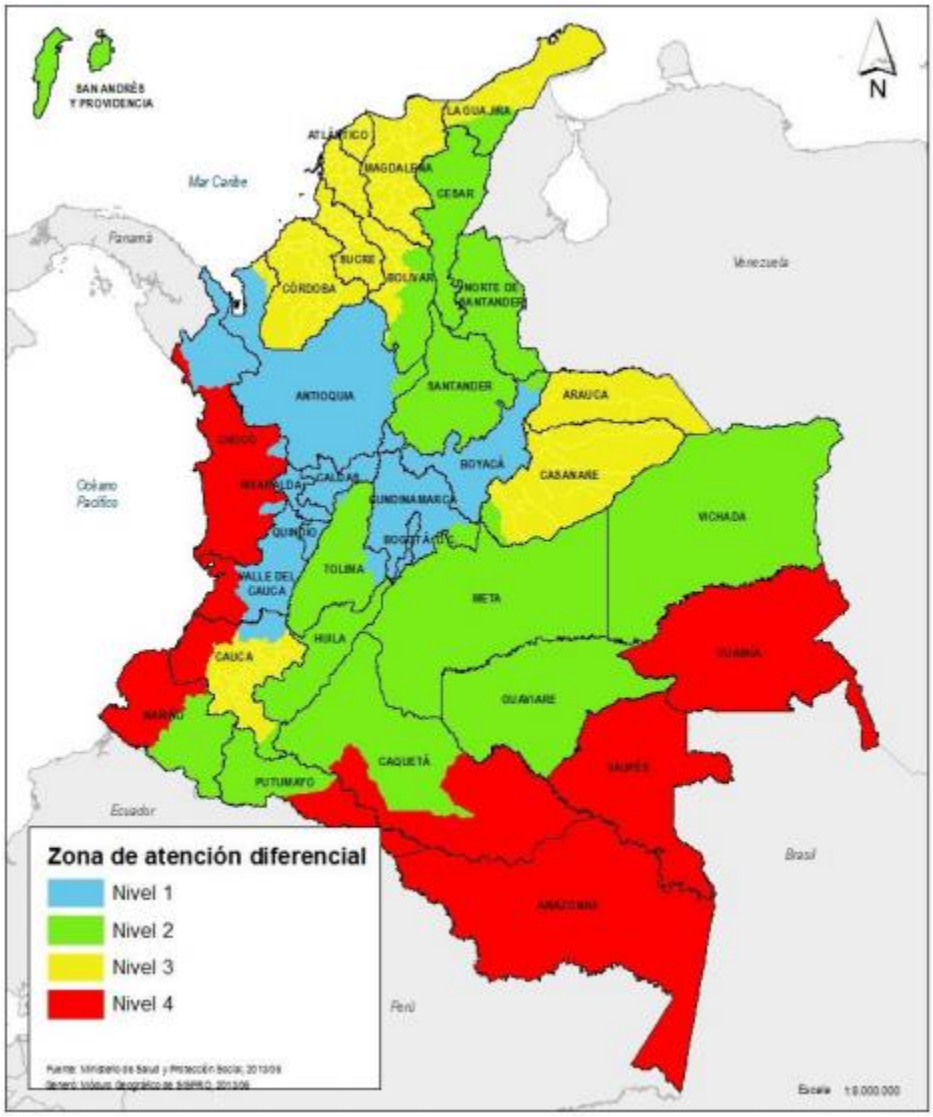
Fuente: Adaptado de la revista (*América Economía*, 2019).

Las empresas del sector salud se encuentran vigiladas y reguladas por el Ministerio de Salud y Protección Social de Colombia, la Superintendencia Nacional de Salud, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima) y la Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES). Además, el sector cuenta con la Asociación Colombiana de Hospitales y Clínicas, entidad gremial sin ánimo de lucro a la cual están afiliadas más de 300 instituciones en el país (Sectorial, 2020). Sin embargo, ninguna de estas entidades realiza vigilancia sobre el sector en temas de seguridad, privacidad y protección de datos. La Superintendencia de Industria y Comercio (SIC), a través de la Delegatura para la protección de datos personales, es la única autoridad a nivel nacional que puede realizar vigilancia en este sentido sobre las empresas del sector salud.

De acuerdo con un estudio sobre geografía sanitaria en Colombia del año 2013 (Páez, Jaramillo, & Franco, 2013) se da una relación entre un mayor nivel de atención en salud y el

desarrollo socioeconómico regional, mostrando que los departamentos de Antioquia, Boyacá, Cundinamarca, Caldas, Quindío, Valle del Cauca y Risaralda se ubican dentro de una zona de atención diferencial de Nivel 1, cuyas características representan mejores condiciones respecto a cobertura, oferta y demanda de salud. De forma contraria, el Nivel 4 representa peores condiciones. Figura 4. Esta información, a la luz de la delimitación geográfica de la propuesta, resulta relevante.

Figura 4. Categorías de atención en zonas de prestación de servicios.

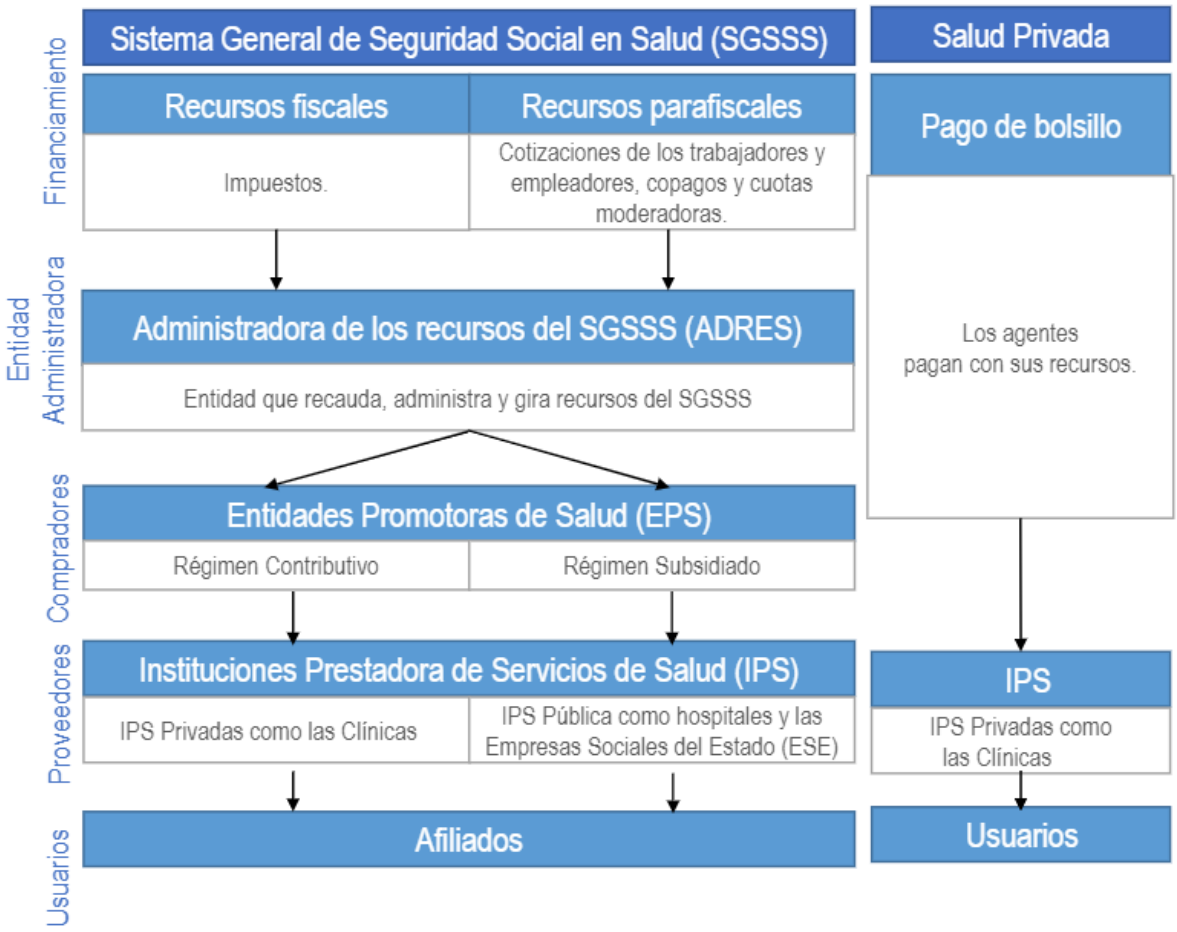


Fuente: (Páez, Jaramillo & Franco, 2013, p. 304)

Cadena de Funcionamiento

El sistema de salud en Colombia se encuentra dividido entre el Sistema General de Seguridad Social en Salud (SGSSS) que cuenta con el régimen contributivo y el subsidiado; y la Salud privada. El SGSSS se rige bajo la ley 100 de 1993 (Secretaria del Senado, 1993) que estableció el derecho de los colombianos a contar con un servicio público de salud. Figura 5.

Figura 5. Estructura del sistema de salud colombiano.



Fuente: (Sectorial, 2020, p. 13)

Los servicios de salud pueden ser de distinta naturaleza y según esta hacen parte o no del Plan de Beneficios en Salud (PBS), que fue establecido por el Ministerio de Salud. Si el servicio de salud al cual quiere acceder un afiliado se encuentra en el conjunto de servicios del PBS, las

EPS deben garantizar su prestación. Esto se da a través de la financiación por Unidad de Pago por Capitación (UPC), que es girada por ADRES a las EPS, previo a los requerimientos de atención por parte de los afiliados (Sectorial, 2020). El Ministerio de Salud es el encargado de definir los valores anuales de la UPC, tanto para el régimen contributivo como para el subsidiado.

Los servicios de salud que se encuentran por fuera del PBS, deben ser financiados por los afiliados o usuarios con sus propios recursos, a excepción que interpongan acción de tutela para que les concedan por parte del Estado acceso a los servicios de salud demandados. A partir de marzo de 2020, se estableció que ADRES giré de forma anticipada los fondos para atender servicios no PBS.

Los ingresos de las empresas del sector provienen de ADRES con el giro de recursos para los regímenes contributivo y subsidiado, las cuotas moderadoras y copagos, que son los aportes que realizan los afiliados del régimen contributivo, el SOAT como seguro para vehículos que transiten en el país utilizado para cubrir daños corporales que se causen a personas en accidentes de tránsito, el sistema general de participaciones, que representan un 24,5% de aportes a salud de acuerdo con lo definido en la ley 715 de 2001 (Secretaria Senado, 2001), las contribuciones patronales correspondientes a las obligaciones del empleador al SGSSS, y las rentas cedidas de loterías, juegos y licores que se utilizan para el pago de servicios fuera del PBS del régimen subsidiado (Sectorial, 2020).

De otra parte, los egresos se representan en costos variables (medicamentos, dispositivos médicos entre otros), mano de obra (personal médico principalmente), investigación y desarrollo, implementaciones tecnológicas, transporte de pacientes y gestión de desechos de residuos peligrosos (Sectorial, 2020).

Por último, los proveedores y clientes que interactúan en el sistema de salud se presentan en la Figura 6.

Figura 6. Proveedores y clientes del sector salud.

Proveedores

Producto / Servicio	Tipo de proveedor
Gases medicinales	Compañías proveedoras de gases medicinales como oxígeno, óxido nitroso, aire medicinal, entre otros
Dispositivos médicos	Compañías proveedoras de artículos, instrumentos, aparatos o máquinas utilizados en la prevención, el diagnóstico o el tratamiento de una enfermedad o condición
Medicamentos	Compañías de la industria farmacéutica
Implementación tecnológica	Compañías proveedoras de soluciones informáticas y tecnológicas
Transporte de pacientes	Compañías de ambulancias
Desecho de residuos peligrosos y biológicos	Compañías dedicadas al manejo de residuos biológicos y peligrosos

Clientes

Producto / Servicio	Tipo de cliente
Atención de usuarios y prestación de servicios PBS y no PBS	Entidades Promotoras de Salud (EPS)
	Seguro Obligatorio de Accidentes de Tránsito
	Pacientes particulares
	Otras IPS

Fuente: (Sectorial, 2020, p. 19)

Como se observa, el sistema de salud en Colombia cuenta con diferentes actores en su cadena de funcionamiento, los cuales en diferentes momentos interactúan con la información de los usuarios y pacientes. Dado que esta información tiene una naturaleza especial respecto a sus necesidades de protección, es importante considerar cuáles son los aspectos claves de análisis desde la seguridad de esta.

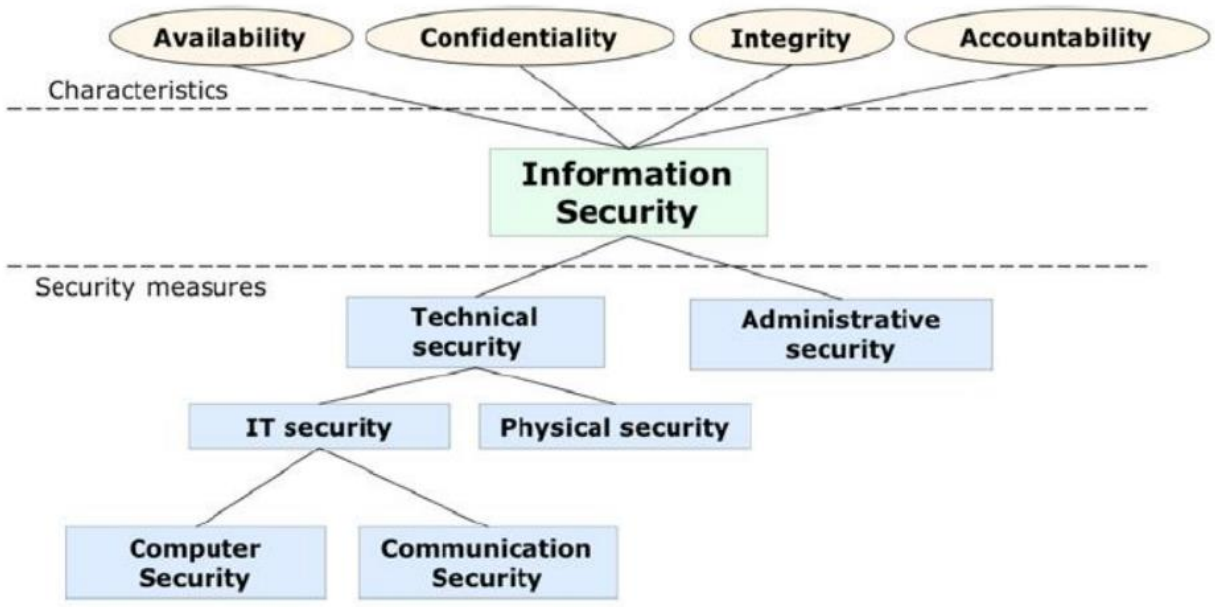
Seguridad de la información

La seguridad de la información referida en algunos casos como seguridad informática (*computer security*), se ha asociado como una disciplina o los procesos (SANS Institute, s.f.; NIST, s.f.; CISCO, s.f.; Mitnick & Simon, 2002) que buscan mantener la confidencialidad, integridad y disponibilidad de la información; estos han sido referidos desde la academia tradicional como la

triada de la seguridad. Bishop (2005) indica que la interpretación de estos tres aspectos varía al igual que en los contextos en los que surgen, y que esas interpretaciones están dictadas por las necesidades de los individuos, las costumbres y las leyes de la organización en particular donde se revise. De acuerdo con Miessler (2018), la seguridad de la información es una disciplina tan amplia que es fácil perderse en una sola área y perder la perspectiva. La disciplina abarca todo, desde la altura a la que se debe construir la cerca fuera de la empresa, hasta cómo reforzar un servidor.

En este sentido, cuando se ha hablado de la seguridad de la información se parte de los conceptos globales de la triada y acorde con la organización o industria donde se esté validando, dichos conceptos son adaptados para las necesidades específicas. La **confidencialidad** es el ocultamiento de la información o los recursos (Bishop, 2005) para personas o entidades no autorizadas y está basado en un principio de necesidad de conocer, cuyo origen fue motivado desde el campo militar. **Integridad** se refiere a la confiabilidad de los datos (exactitud) expresada como prevención ante cambios no autorizados (Bishop, 2005). Por último, la **disponibilidad** es la accesibilidad de la información o los recursos cuando son requeridos por la persona o entidad autorizadas (Lundgren & Möller, 2019). Con esto se busca proteger la información confidencial, privada o sensible de los negocios en formato impreso o electrónico de modificación, divulgación, interrupción, destrucción, acceso o uso no autorizado. Adicional a estos conceptos, en seguridad se maneja el termino de **trazabilidad** para hacer referencia a la propiedad de asegurar que las acciones de una entidad se pueden rastrear inequívocamente (NIST, s.f). La Figura 7 presenta las características de la seguridad y su relación con las medidas de seguridad a implementar para su protección, acorde con el modelo de seguridad basado en SIS – *Sensitive Information Security*.

Figura 7. Modelo de seguridad de la información basado en el modelo SIS



Fuente: Åhlfeldt R. M., 2008, p. 36.

Seguridad de la información en el Sector Salud

Para el sector de la salud, la información está representada en los datos de pacientes (historias clínicas, registros médicos, datos personales, datos de pago, entre otros), clientes, personal médico y administrativo, así como la información de procesos y servicios de las empresas prestadores de servicios de salud y sus aliados de negocio (proveedores y terceros en la cadena de valor) que en formato físico o electrónico son procesados para la prestación de estos. Por lo anterior, los conceptos de seguridad de la información se aplican al sector de la salud en términos de proteger estos datos de modificación, divulgación, destrucción o acceso no autorizado.

Adicional a la triada de seguridad de la información, en el campo de la salud se realiza énfasis en el principio de **privacidad** que ha sido adoptado desde enfoques constitucionales y normativos por las naciones, al considerar como derecho legal la privacidad individual, con lo cual

las personas pueden mantener reserva sobre información de identificación personal (por sus siglas en inglés *Personal Identifiable Information* abreviado PII) que se considera de carácter sensible. Dentro de esta categoría se encuentra la información médica.

Las instituciones prestadoras de servicios de salud, así como los proveedores y terceros en la cadena de valor, presentan debilidades (Åhlfeldt & Söderström, 2008) (Fernández-Alemán, Carrión, Oliver, & Toval, 2013; Mahmood, 2010) asociadas a la no disponibilidad de la información de pacientes dentro de la institución, ausencia de logs de auditoria y monitoreo constante que se considera costoso, ausencia de regulación para el cifrado de información dentro de las instituciones que proveen servicios, falta de conocimiento sobre el nivel de seguridad de las aplicaciones, inadecuada seguridad física, deficiencias técnicas y administrativas, nuevas amenazas por uso de registros médicos electrónicos, ausencia de estandarización de medidas de seguridad entre empresas prestadoras de salud, falta de relevancia en el entrenamiento a personal en seguridad y privacidad, e incluso falta de toma de conciencia dirigida a los mismos pacientes.

Por lo anterior, la información médica y las entidades del sector salud se encuentran expuestas a riesgos de seguridad de la información como se presentan en la Tabla 10.

Tabla 10. Riesgos de seguridad para la información médica y las entidades de salud

Riesgo	**Autores**
Acceso no autorizado a la red, por temas como no asegurar la *WiFi*	(Chen & Benusa, 2017), (Davidson & Lambert, 2004), (Fatima & Colomo-Palacios, 2018)
Pérdida de equipos y dispositivos de almacenamiento (laptops, móviles y USB)	(Chen & Benusa, 2017)

Infección por malware	(Chen & Benusa, 2017), (Subramoniam & Sadi, 2010), (Fatima & Colomo-Palacios, 2018)
Acceso/Uso no autorizado a registros médicos (por internos o externos)	(Chen & Benusa, 2017), (Subramoniam & Sadi, 2010), (Gand, 2017), (Fatima & Colomo-Palacios, 2018), (Abila, Kemboi, & Ronoh, 2019)
Pérdida de datos por falla de dispositivos de almacenamiento	(Chen & Benusa, 2017), (Fatima & Colomo-Palacios, 2018)
Uso no adecuado de información médica por terceras partes	(Subramoniam & Sadi, 2010), (Fatima & Colomo-Palacios, 2018)

Fuente: Elaboración propia a partir de los autores mencionados.

Como lo indica Mahmood (2010), diariamente un gran número de pacientes interactúan con diferentes actores de la salud (doctores, enfermeras, farmacéuticas, y otros trabajadores de la salud) y los resultados médicos son comunicados y gestionados a través de sistemas tecnológicos de salud. Por lo anterior, deben existir mecanismos y estructuras organizadas para almacenar, gestionar, y proteger esta información de amenazas. Por ello, se requieren conciencia en la protección por parte de las entidades, así como normativa que les exija a estas la protección de la información médica.

A nivel mundial se ha fortalecido la legislación y normativa desde la óptica de la seguridad y privacidad de datos personales. No obstante, aún se presentan falencias en este aspecto para los países que se encuentran en vía de desarrollo (tal como es el caso de Colombia) de forma tal que se favorezca la protección de la información médica y que se exija a las empresas prestadoras de servicios de salud y sus socios de negocio proteger esta. Países como Estados Unidos han generado legislación específica (por ejemplo, HIPAA) para la protección de la información médica, sin embargo, en la mayoría de los países la fuente más cercana de legislación para proteger los datos

médicos se encuentra enmarcada en las leyes de protección de datos personales. En la Tabla 11 se presenta la legislación de mayor relevancia que se encuentra vigente actualmente.

Tabla 11. Legislación relacionada con seguridad y privacidad para el sector salud.

País	**Legislación**	**Descripción / Objetivos**	**Fuente**
Estados Unidos	HIPAA - *The Health Insurance Portability and Accountability Act* (1996)	Tiene como objetivos asegurar que las personas puedan mantener sus seguros entre trabajos, y mantener la confidencialidad y seguridad de la información de pacientes.	(HHS, s.f.)
	HITECH - *Health Information Technology for Economic and Clinical Health* (2009)	Modifica reglas de HIPAA para fortalecer el cumplimiento de la privacidad y seguridad.	(HealthIT, s.f.)
Europa (Unión Europea)	GDPR - *General Data Protection Regulation* (2016)	Buscar proveer un conjunto estandarizado de leyes de protección de datos para los países miembro.	(EUR-Lex, s.f.)
Canadá	*The Privacy Act* (1983)	Gobierna las prácticas de gestión de información personal de las instituciones de gobierno federal.	(Government of Canada, 1985)
	PIPEDA - *The Personal Information Protection and Electronic Documents Act* (2004)	Reglas para gestionar la información personal, reconociendo el derecho a la privacidad.	(Government of Canada, 2000)
Colombia	Ley 1581 sobre protección de datos personales (2012)	Desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar su información personal.	(Función Pública, s.f.)
Estonia	The Health Services Organization Act (2002)	Incluye reglas de protección de datos requeridas para la atención médica.	(Riigi Teataja, 2018)

Francia	Law n° 2018-493 (2018)	Protección de datos personales	(République Francaise, 2018)
Alemania	*Law for Patient Data Protection* (2020) *Regulation on the Requirements and Reimbursement Process for Digital Health Applications* (2020)	Buscar aumentar el uso de aplicaciones digitales, mientras protege los datos confidenciales de salud. Incluye requerimientos específicos de seguridad de TI y privacidad.	(iapp, 2020) (Elteste, Van Quathem, & Oberschelp de Meneses, 2020)
Irlanda	*IHI Service Data Protection Policy* (2014)	Proporcionar orientación e instrucciones a quienes manejan datos de salud sobre la forma adecuada, segura y legal en que pueden usar esta información.	(Head of HSE IHI Business Service, 2017)
Israel	*Protection of privacy regulations (data security) 5777-2017* (2018)	Aplica para sector público y privado y establece los mecanismos destinados para que la seguridad forme parte de las rutinas de gestión de las organizaciones que procesan datos personales.	(The Privacy Protection Authority, 2021)
Japón	APPI - *Act on the Protection of Personal Information* (Act No. 57 of 2003)	Proteger los derechos e intereses de las personas mientras se considera la protección de la información personal.	(Cabinet Secretariat, s.f.)
México	*Federal Law on the Protection of Personal Data Held by Private Parties* (2011)	Regular las disposiciones para la protección de los datos personales realizada por terceros.	(iapp, s.f.)
Países Bajos	PDPA - *Personal Data Protection Act (Wet bescherming persoonsgegevens)* (2016)	Protección de datos personales.	(Library of Congress, s.f.)
Qatar	*Law No. 13 on the Protection of Personal*	Impone obligaciones a individuos y entidades que recopilen y procesen	(Squire Patton Boggs, s.f.)

	Data and Privacy (2016)	electrónicamente datos personales.	
Rusia	*Federal Law of 27 N 152-FZ on personal data* (2006)	Regula las actividades relacionadas con el procesamiento de datos personales por las entidades federales.	(The Federal Servie for Supervision of Communications, Information Technology, s.f.)
Suecia	DPA - *The Data Protection Act (2018:218)*	Regula los aspectos generales de protección de datos.	(The Swedish Data Protection Authority, s.f.)
Suiza	DPA - Federal Act on Data Protection (1992)	Regulación sobre protección de datos.	(Federal Data Protection and Information Commissioner (FDPIC), s.f.)
Reino Unido	DPA - Federal Act on Data Protection (2018)	Regulación sobre protección de datos.	(legislation.gov.uk, 2018)

Fuente: Elaboración propia a partir de las fuentes citadas.

Teniendo en cuenta como la seguridad de la información desde la perspectiva de la privacidad, permite dar alcance a la protección de la información personal, incluyendo la información médica, a continuación se explica el concepto de modelos de negocio con el fin de sustentar cómo, a través de estos se puede generar una propuesta de valor de servicios de seguridad de la información, cuyo interés principal es proteger la información médica.

Modelos de Negocio

Los modelos de negocio permiten explicar la estrategia organizacional, hablar de arquitectura organizacional y pueden actuar como mecanismo de generación de valor para clientes y la organización bajo una vista estratégica competitiva. Acorde con la investigación de Gomes & Moqaddemerad (2016) el concepto de modelo de negocio es definido desde diferentes perspectivas para hablar de la proliferación de negocios, como se presenta en la Tabla 12.

Tabla 12. El concepto de modelo de negocio.

Perspectiva del concepto	**Autores**
Como una descripción	(Applegate, 2000; Weill & Vitale, 2001)
Como una arquitectura	(Timmers, 1998; Dubosson-Torbay, Osterwalder, & Pigneur, 2002)
Como una representación	(Morrisa, Schindehutteb, & Allen, 2005; Shafer, Smith, & Linder, 2005)
Como un modelo o herramienta conceptual	(Osterwalder A. , 2004); (Osterwalder, Pigneur, & Tucci, 2005)
Como una plantilla estructural	(Amit & Zott, 2001)
Como un método	(Afuah & Tucci, 2001)
Como una receta	(Baden-Fuller & Morgan, 2010)
Como un *framework*	(Afuah A. , 2004)
Como un conjunto	(Seelos & Mair, 2007)

Fuente: Adaptado de (Gomes & Moqaddemerad, 2016, p. 4).

De otra parte, para el diseño de los modelos de negocio en la literatura se proponen diferentes marcos conceptuales y ontologías, como se presenta en la Tabla 13.

Tabla 13. Marcos conceptuales y ontologías para diseño de modelos de negocio.

Marco conceptual u ontología	**Autor(es)**
Ontología del modelo de negocio (*Business Model Ontology* - BMO)	(Osterwalder A. , 2004)
Modelo Servicio, Tecnología, Organización y Finanzas (*Service, Technology, Organization and Finance* - STOF)	(Bouwman, De Vos, & Haaker, 2008)
Modelo Cliente, Servicio, Organización, Tecnología y Finanzas (*Customer, Service, Organization, Technology, and Finance* – CSOFT)	(Heikkilä, Tyrväinen, & Heikkilä, 2010)
Modelo Propuesta de valor, Interfaces, Plataformas de servicio, Modelo de organización y Modelo de ingresos (*Value proposition, Interfaces, Service platforms, Organising model, and Revenue model* – VISOR), cuyos componentes son comparables con los de STOF	(El Sawy & Pereira, 2013)
e^3-value	(Gordijn & Akkermans, 2001)
Ontología del agente de eventos de recursos (*Resource event agent* - REA)	(McCarthy, 1982)

Modelo de negocios de 4 cajas (*Four-Box Business Model*) donde cada caja representa la propuesta de valor al cliente (CVP)	(Johnson, Christensen, & Kagermann, 2008)
Fórmula de ganancias, recursos y procesos claves, el modelo de negocio de componentes de IBM.	(Tian, Ray, Lee, Cao, & Ding, 2008)
Modelo de negocio conceptual de los autores en el que proponen la inclusión de clientes, competidores, oferta, actividades y organización, recursos e interacciones del mercado.	Hedman & Kalling (2003)
Modelo propuesto por los autores que integra y sintetiza componentes de estrategia, red de valor, creación de valor y captura de valor.	Shafer, Smith & Linder (2005)
Modelo de negocio Canvas que contempla nueve módulos (segmento de mercado, propuestas de valor, canales, relaciones con los clientes, fuentes de ingresos, recursos clave, actividades clave, asociaciones clave, estructura de costes) y que de acuerdo con los autores reflejan la lógica que siguen las empresas para conseguir ingresos.	Osterwalder & Pigneur (2011)

Fuente: Elaboración propia a partir de los autores referidos.

El modelo de Osterwalder y Pigneur (2011) en su estructura agrupa y condensa varios de los componentes planteados por los modelos de negocio de los otros autores revisados y facilita su análisis cubriendo las áreas principales de los negocios: clientes, oferta, infraestructura y viabilidad económica, por tales motivos ha sido el modelo seleccionado para aplicar en este trabajo. En la Tabla 14 se presentan los componentes del Canvas.

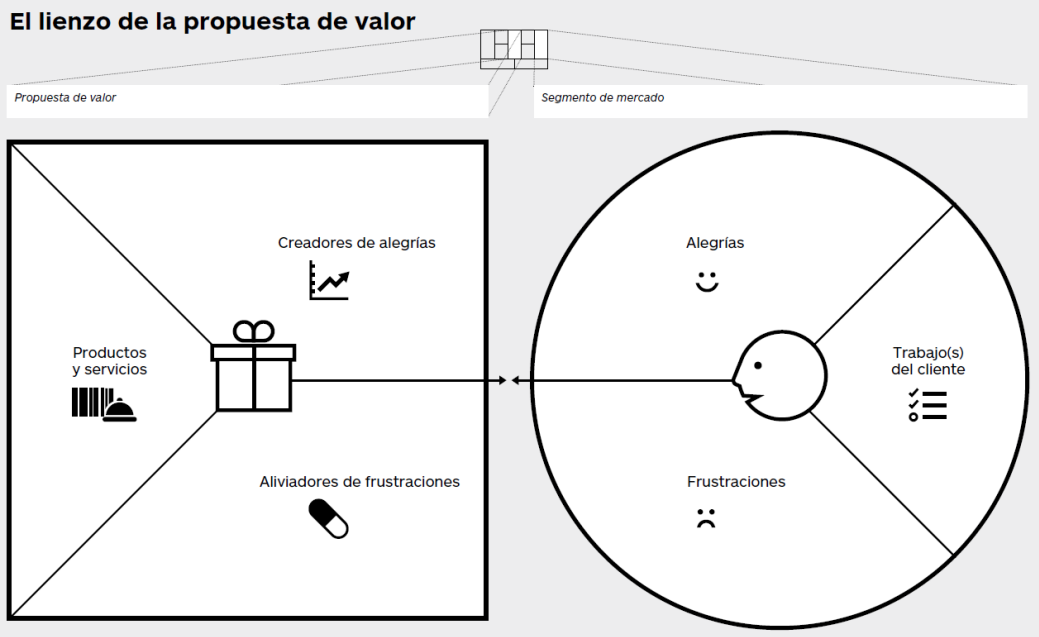
Tabla 14. Componentes del Canvas de Osterwalder y Pigneur (2011)

Componente (Módulo)	**Descripción**
Segmentos del mercado	Una empresa atiende a uno o varios segmentos de mercado. Los segmentos de mercado son los grupos de personas o entidades a los que se dirige la empresa.
Propuestas de valor	Su objetivo es solucionar los problemas de los clientes y satisfacer sus necesidades de los segmentos de mercado.
Canales	Las propuestas de valor llegan a los clientes a través de canales de comunicación, distribución y venta.
Relaciones con clientes	Las relaciones con los clientes se establecen y mantienen de forma independiente en los diferentes segmentos de mercado.
Fuentes de ingresos	Las fuentes de ingresos se generan cuando los clientes adquieren las propuestas de valor ofrecidas.
Recursos clave	Los recursos clave son los activos necesarios para ofrecer y proporcionar los elementos antes descritos.
Actividades clave	Las actividades clave, junto con los recursos clave permiten generar y ofrecer la propuesta de valor.
Asociaciones clave	Algunas actividades se externalizan y determinados recursos que se adquieren fuera de la empresa.
Estructura de costes	Los diferentes elementos del modelo de negocio conforman la estructura de costes, es decir, son los costos de la puesta en marcha del modelo de negocio.

Fuente: (Osterwalder & Pigneur, 2011, pp. 16-40).

En igual medida, para detallar el perfil del segmento de mercado y la propuesta de valor se toma como referencia el lienzo de la propuesta de valor (Osterwalder A. , Pigneur, Bernarda, & Smith, 2014) donde se detallan los trabajos, alegrías y frustraciones del cliente, así como los creadores de alegrías, los aliviadores de frustraciones y los productos y servicios con los cuales se construye la propuesta de valor. Figura 8.

Figura 8. Lienzo de la propuesta de valor



Fuente: (Strategizer, s.f.).

A continuación, en la Tabla 15, se describen cada uno de los componentes del lienzo de la propuesta de valor.

Tabla 15. Componentes del lienzo de la propuesta de valor

Componente	**Descripción**
Trabajos del cliente	Describen lo que intentan resolver los clientes
Alegrías	Se refieren a los resultados que quieren conseguir los clientes o beneficios concretos que buscan
Frustraciones	Se refieren a los malos resultados, riesgos y obstáculos relacionados con los trabajos
Creadores de alegrías	Describen cómo, con los productos y servicios de la oferta de valor, se cubren las alegrías del cliente
Aliviadores de frustraciones	Describen cómo, con los productos y servicios de la oferta de valor, ayudan a cubrir las frustraciones del cliente
Productos y servicios	Considera aquello con lo cual se construye la propuesta de valor

Fuente: Adaptado de (Osterwalder, Pigneur, Bernarda & Smith, 2014, pp. 38-39).

Una vez se cuenta con el marco conceptual, en el siguiente apartado se presenta el proceso metodológico a partir del cual se realizó la revisión de literatura que sirvió como base para el planteamiento del modelo de negocio de seguridad de la información propuesto en este trabajo.

Proceso Metodológico

Con el objetivo de proponer un modelo de negocio de seguridad de la información para Pymes del sector salud, esta investigación se realiza con un enfoque exploratorio y un análisis cualitativo, para ello se consideran tres etapas: La primera corresponde a una **búsqueda y revisión de literatura** guiada por las preguntas: ¿qué debe tener una propuesta de servicios de seguridad de la información que se adapte a las limitaciones y necesidades que tienen las Pymes colombianas? y ¿qué debe tener la propuesta de servicios de seguridad de la información que se adapte a las limitaciones y necesidades de Pymes en el sector salud? La segunda, considera el **análisis de los conceptos centrales identificados en la revisión de la literatura** que aportan para la construcción de los elementos del modelo de negocio. La etapa final corresponde con el **planteamiento del modelo de negocio a partir de los elementos encontrados en las investigaciones identificadas en la revisión de literatura** y una propuesta desde la experiencia del autor de este texto sobre prestación de servicios de seguridad de la información a empresas del sector de la salud.

Etapa I - Búsqueda y revisión de literatura

En esta etapa se realizó consulta desde *Google Scholar* utilizando los términos: "*business model*", "*healthcare*", "*SME – Small and Medium Enterprise*" e "*information security*". A partir de los términos anteriores se consultaron variaciones de términos como "*information security business model*", "*business model for information security*" e "*information security in healthcare*" en el título. La búsqueda se limitó a publicaciones en inglés o español, identificando un total de 704 textos (ver Tabla 16). El periodo para la revisión se tomó entre 2000-2020 con el fin de poder

identificar a partir de qué momento se empieza a reconocer el concepto de seguridad de la información en el campo de la salud.

Tabla 16. Criterios de búsqueda de artículos académicos y de investigación.

Criterio de búsqueda	**Cantidad de artículos**
Information security business model	8
Business model for information security	375
Information security in healthcare	311
"Business model" AND "healthcare SMEs"	10

Fuente: Elaboración propia.

A partir de los resultados anteriores se realizó la revisión del *abstract* y las palabras claves. Algunos artículos no fueron accesibles desde *Google Scholar*, por lo cual su búsqueda se realizó desde las bases de datos de EAFIT. Luego, se definieron los siguientes criterios de exclusión: 1) manejo de enfoque únicamente en la adopción de tecnologías en el sector salud, 2) campos específicos de seguridad de la información como seguridad en la nube, 3) conceptos de innovación en modelos de negocio, 4) aspectos en relación con *SMEs* orientados a múltiples industrias que pierden el foco en salud, y, 5) artículos de conferencias y simposios. Finalmente se obtuvieron 46 artículos sobre los cuales se realizó una revisión rigurosa de la literatura (ver Anexo 1).

Con la revisión de literatura fue posible resaltar que hasta el año 2020 (fecha final del período de revisión de la literatura) no se encontraron planteamientos específicos de modelos de negocio en seguridad de la información aplicados a Pymes del sector salud, lo cual a priori permite identificar una oportunidad asociada a la pregunta de investigación. Incluso bajo la denominación

de modelo de negocio para seguridad de la información, únicamente ha sido trabajado un modelo por la asociación ISACA (*Information Systems Audit and Control Association)* con el nombre BMIS – *Business Model for Information Security,* que considera la integración de procesos, personas, tecnología y organización para el despliegue de seguridad de la información dentro de las empresas.

Otro aspecto relevante que se identifica en la revisión es que las investigaciones y planteamientos que han sido realizados para incluir seguridad de la información como parte de los modelos de negocio y operación en las empresas del sector de la salud, han sido explorados en su mayoría fuera de Latinoamérica, lo cual también brinda una oportunidad para su estudio desde la región. Este análisis se presenta en la Tabla 17.

Tabla 17. Publicaciones consultadas por regiones.

Numero de publicaciones	Región (Países)
21	Europa (Alemania, Austria, Bélgica, Dinamarca, Eslovenia, España, Finlandia, Grecia, Italia, Noruega, Reino Unido, Serbia, Suecia, Suiza)
13	Norteamérica (Canada, Estados Unidos)
4	África (Ghana, Kenia, Marruecos, Nigeria)
3	Oceania (Australia)
3	Asia (India, Malaysia)
2	Latino America (Brazil, Ecuador)

Fuente: Elaboración propia.

Etapa II - Análisis de fuentes documentales

A partir de la lectura y el análisis de los documentos seleccionados de la etapa anterior, fueron tomados datos sobre investigaciones relacionados con los modelos de operación de las empresas prestadoras de servicios de salud, la operación de seguridad de la información en estas empresas, la adopción de tecnologías de la información (ICT por sus siglas en inglés) por estas empresas y las implicaciones desde seguridad, los riesgos a los cuales se puede ver expuesta la información médica, la importancia de protegerla y algunas medidas o controles propuestos para realizar esta protección.

Estos elementos son tomados como puntos de referencia para la construcción de la propuesta de los módulos del Canvas (segmentos de mercado, propuesta de valor, canales, relación con los clientes, fuentes de ingresos, recursos clave, actividades clave, asociaciones clave y estructura de costos) en la etapa 3.

Etapa III – Planteamiento del modelo de negocio

En esta etapa son sintetizados e integrados los elementos identificados en la revisión de la literatura, junto con el análisis de los requerimientos en seguridad de la información que pueden ser aplicables a las Pymes de salud en Colombia. Con lo anterior se busca responder a la pregunta de investigación con el diseño de un modelo de negocio de seguridad de la información adaptado al sector de Pymes de salud en el país, basado en el lienzo de modelo de negocio Canvas, bajo el cual se presentan los elementos claves que desde el campo de seguridad de la información se pueden brindar a las Pymes de salud para adoptar este como parte de su esquema de operación y con ello aportar a la seguridad de los pacientes y la privacidad de su información.

Investigaciones en seguridad de la información en Pymes y para el sector salud

Como resultado de la revisión de los 46 documentos seleccionados para su análisis en profundidad y obtención de datos relevantes para la construcción de los módulos del modelo de negocio, se identificaron los temas claves presentados en la Tabla 18.

Tabla 18. Temas de investigación identificados en los artículos revisados.

Tema	**Autor(es), Año**
Impacto de las tecnologías de la información en SMEs y riesgos asociados a su uso	Okundaye, et al., 2019; Gomes & Moqaddemerad, 2016; Subramoniam & Sadi, 2010; Stanimirovic, 2015; Yang, 2018; Prince & King, 2012; Cook, 2017; Patterson, 2017; Matrane & Talea, 2014; Vassilis, et al., 2004.
Innovación en SMEs	Stanković, Djukić, & Lepojević, 2014; Heikkilä, Bouwman, & Heikkilä, 2018;Kriegel, Riedl, Tuttle-Weidinger, & Stöbich, 2020.
Modelos de negocio y creación de valor desde la perspectiva de SMEs y el sector salud	Svetla, Jorma & Niina, 2016; Cicellin, et al., 2019; Bohnet-Joschko, et al., 2019; Gand, 2017.
Controles de seguridad de la información en servicios de salud	Kissi, et al., 2018; Armstrong, 2000; Hassan & Ismail, 2012; Söderström, Åhlfeldt & Eriksson, 2009; Wallin &Ying, 2008; Cooper & Collman, 2005; Fatima & Colomo-Palacios, 2018; Åhlfeldt & Söderström, 2008; Narayana, Naik & Venkataiah, 2013; Fernández, et al., 2013;Onyango, Kemboi & Lamek, 2019; Mahmood, 2010; Public Health Emergency, 2017; Healthcare Information and Management Systems Society, 2019 y 2020.
Servicios de seguridad orientados a Pymes	Zambrano, 2015; Bahl, Wali & Kumaraguru, 2011.
Legislación y estándares en seguridad de la información para SMEs y en el sector salud	Chen & Benusa, 2017; Robyn & Lambert, 2004; Appari & Johnson, 2010; Galan, Rekleitis, Papazafeiropoulos, & Maritsas, 2015; Paulsen & Toth, 2016; European Digital SME Alliance, 2019 y 2020; Canadian Centre for Cybersecurity, 2020.

Modelos de negocio en seguridad de la información	Von Roessing, 2010; Williams, 2013; Alshboul & Streff, 2015; Da Silva Neto, Dias & Lira, 2015; ISACA, 2010.

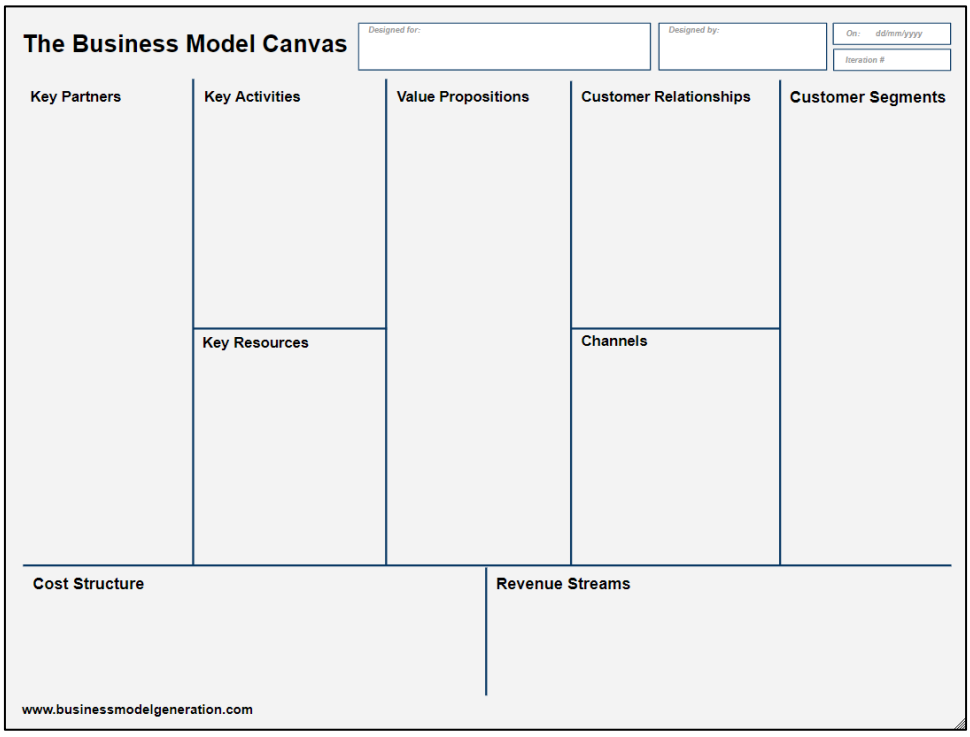
Fuente: Elaboración propia.

Con la información obtenida previamente, en el siguiente apartado se presenta el modelo de negocio en seguridad de la información para Pymes del sector salud en Bogotá, tomando como referencia los elementos obtenidos en la revisión de literatura para la identificación del segmento de mercado objetivo, la propuesta de valor, los canales, el esquema de relacionamiento con el cliente, el modelo de ingresos, así como las actividades y recursos clave para llevar la propuesta de valor, asociaciones clave requeridas y la estructura de costos que soporte el modelo.

Propuesta de lienzo de modelo de negocio en seguridad de la información para Pymes del sector salud en Bogotá - Colombia

Partiendo del concepto de Osterwalder y Pigneur (2011), en el cual el modelo de negocio describe las bases sobre las cuales una empresa crea, proporciona y captura valor, en este capítulo se propone un modelo de negocio en seguridad de la información, orientado a las Pymes del sector salud en Colombia con una descripción a partir del planteamiento de los 9 módulos básicos del Canvas (segmentos de mercado, propuesta de valor, canales, relaciones con clientes, fuentes de ingresos, recursos clave, actividades clave, asociaciones clave y estructura de costes) presentados en la Figura 9 con el fin de dar cubrimiento a las principales áreas de negocio clientes, oferta, infraestructura y viabilidad económica.

Figura 9. Módulos modelo de negocio Canvas



Fuente: (Strategizer, s.f.)

Cada uno de los módulos clave son descritos a continuación, presentando su construcción a partir de los elementos identificados en la revisión de literatura, considerando necesidades y requerimientos de los clientes objetivos, limitaciones del sector salud, amenazas y riesgos en seguridad de la información identificados para ellos y las oportunidades actuales y futuras relacionadas con la adopción de tecnologías de la información y su impacto en los requerimientos de la información médica.

Segmentos de mercado

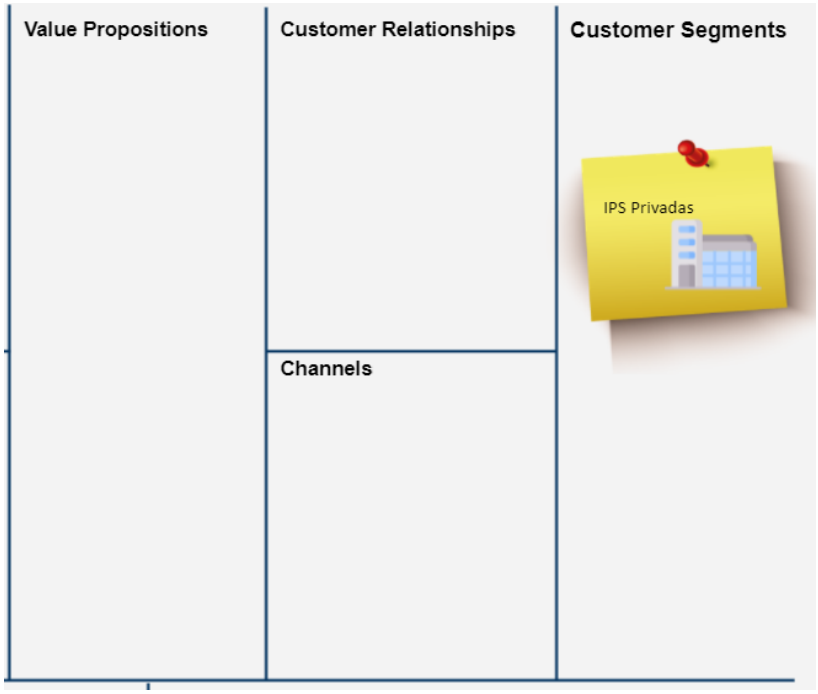
Para definir el segmento de mercado al cual será dirigido el modelo de negocio que se construye en este trabajo, se inicia desde la cadena de funcionamiento del sector salud presentada en el marco conceptual. La delimitación para su selección parte de los siguientes preceptos respecto a los actores que intervienen en la cadena: 1) cuál es el alcance del actor en la gestión de información médica, 2) cuál es su posición en la cadena de funcionamiento, 3) si la relación es directa o indirecta en la prestación de servicios a los usuarios finales y 4) requisitos de cumplimiento en seguridad y privacidad de la información.

Con lo anterior se aclara y diferencia el alcance frente a quienes se consideran potenciales clientes de este modelo de negocio. Son clientes potenciales las empresas que prestan servicios de salud directa o indirectamente a pacientes, afiliados o usuarios de servicios de salud y/o aquellas empresas aliadas o proveedoras que hacen parte de la cadena de funcionamiento con servicios o productos complementarios, tales como transporte de emergencia, medicamentos o exámenes clínicos. Es decir, los pacientes, afiliados o usuarios finales no son el público objetivo de este modelo de negocio, dado que no son directamente los responsables de la protección de la información médica, sino, que son los beneficiados finales de la implementación de las medidas de protección sobre la información médica.

Con lo anterior se consideraron inicialmente como posibles segmentos de clientes las entidades promotoras de salud – EPS, las instituciones prestadoras de servicios de salud – IPS (públicas o privadas), las compañías de ambulancias, los laboratorios clínicos y las farmacéuticas. A partir de estos se analizaron los preceptos presentados previamente, identificando que las EPS no brindan servicios directamente a pacientes, sino que lo realizan a través de las IPS públicas y/o privadas, por lo cual, aunque tienen acceso a información médica por pertenecer al Sistema General de Seguridad Social en Salud, actúan como compradores de los servicios en un nivel de control más no son prestadores de estos. Este es un primer punto para descartarlas, junto con el concepto que, dada su ubicación en la cadena de funcionamiento, llegar a estas empresas para presentar y tener la oportunidad de prestar los servicios incluidos en la propuesta de valor puede resultar más difícil.

En segunda instancia se analizaron las IPS, identificando que son las empresas que manejan directamente la prestación de servicios hacia pacientes y desde aquí puede desprenderse en gran medida el uso de servicios y productos complementarios como el transporte de emergencia, requerimientos de exámenes clínicos y la formulación de medicamentos. De otra parte, se consideran las IPS privadas, dado que los canales de contacto y acceso a estos pueden ser menos complejos que en el caso de las públicas, donde implicaría necesariamente procesos de contratación estatal. Con lo anterior, las instituciones prestadoras de servicios de salud – IPS privadas son el segmento de mercado específico al cual se dirigirá la propuesta de valor (Figura 10).

Figura 10. Segmento de clientes



Fuente: elaboración propia.

Para este segmento de mercado se analizaron los trabajos, alegrías y frustraciones que pueden ser cubiertas con la propuesta de valor a partir de creadores de alegrías, aliviadores de frustraciones, y productos y servicios, esto corresponde con el perfil del cliente presentado en el lado derecho del lienzo de la propuesta de valor.

Los trabajos del cliente se identificaron a partir de las necesidades de las empresas de salud respecto a seguridad y privacidad de la información encontradas en la revisión de literatura. Estas son presentadas en la Tabla 19.

Tabla 19. Necesidades de las empresas de salud respecto a seguridad

Necesidades en seguridad	**Autor(es)**
Identificar y analizar riesgos de seguridad	(Åhlfeldt & Söderström, 2008), (Dimopoulos, Furnell, Jennex, & Kritharas, 2004), (European Digital SME Alliance, 2020)
Enfocarse más en protección y cuidado del paciente por encima de su privacidad	(Åhlfeldt & Söderström, 2008)
Cumplir con requerimientos legales de proteger la información del paciente respecto a seguridad y privacidad (confidencialidad, integridad, disponibilidad)	(Åhlfeldt & Söderström, 2008)
Asegurar que solo quien requiera acceso a la información médica, sea quien tenga acceso	(Åhlfeldt & Söderström, 2008)
Tener conciencia de seguridad en la empresa	(Åhlfeldt & Söderström, 2008), (Yaping, 2018), (Fatima & Colomo-Palacios, 2018)

Fuente: Elaboración propia a partir de las fuentes citadas.

Como se identifica, el análisis de riesgos es una de las necesidades en las que confluyen varios autores. Su aplicación directa a las IPS privadas considera establecer prioridades y hacer que la implementación de medidas de seguridad sea práctica, dado que no es posible lograr seguridad completa y es necesario considerar que esta debe ser realista a la naturaleza de la empresa. El problema de la seguridad es multifacético, multicapa y de gran magnitud (European Digital SME Alliance, 2020) por ello debe verse con estas perspectivas. Sin embargo, una limitante para que las mismas IPS privadas ejecuten este trabajo en particular se relaciona con la ausencia de tiempo para su realización (Åhlfeldt & Söderström, 2008) y el considerar que si este se ejecuta puede detener la operación (Dimopoulos, et al., 2004). Estos últimos puntos se pueden considerar como frustraciones del cliente.

Otras frustraciones del cliente que pueden ser obtenidas a partir del análisis de las debilidades de las empresas de salud frente a seguridad y los elementos que preocupan a estas, se presentan como elementos en la Tabla 20.

Tabla 20. Frustraciones del cliente

Debilidades (frustraciones) frente a seguridad	**Autor(es)**
Los empleados son el eslabón más débil para seguridad (no tienen entrenamiento en seguridad, abuso de privilegios, poco personal de TI sin conocimiento de seguridad).	(Åhlfeldt & Söderström, 2008), (Fernández-Alemán, Carrión, Oliver, & Toval, 2013), (Abila, Kemboi, & Ronoh, 2019), (Ashrafullah Khalid, 2010), (Dimopoulos, Furnell, Jennex, & Kritharas, 2004), (Fatima & Colomo-Palacios, 2018)
No poder tener logs de auditoria y que estos sean estandarizados entre entidades, monitoreo constante por ser costoso, aunque sea necesario.	(Åhlfeldt R. M., 2008), (Åhlfeldt & Söderström, 2008), (Fernández-Alemán, Carrión, Oliver, & Toval, 2013)
Médicos que se muestran reacios a pedir consentimiento para el uso de información, falta de estandarización frente a consentimientos y regulación.	(Åhlfeldt & Söderström, 2008), (Fernández-Alemán, Carrión, Oliver, & Toval, 2013)
Falta de conocimiento sobre el nivel de seguridad de las aplicaciones que tienen.	(Åhlfeldt & Söderström, 2008), (Ashrafullah Khalid, 2010), (Dimopoulos, Furnell, Jennex, & Kritharas, 2004),
Inadecuada seguridad física.	(Åhlfeldt & Söderström, 2008)
Nuevas amenazas por el uso de registros médicos electrónicos.	(Fernández-Alemán, Carrión, Oliver, & Toval, 2013), (Ashrafullah Khalid, 2010)
Ausencia de definición global de roles de profesionales de salud y técnicos.	(Fernández-Alemán, Carrión, Oliver, & Toval, 2013)
Deficiencias técnicas y administrativas (falta de políticas formales de seguridad).	(Ashrafullah Khalid, 2010), (Dimopoulos, Furnell, Jennex, & Kritharas, 2004)

Escasa inversión en seguridad (limitación de recursos)	(Dimopoulos, Furnell, Jennex, & Kritharas, 2004)
No saber dónde empezar en seguridad	(Dimopoulos, Furnell, Jennex, & Kritharas, 2004), (Yaping, 2018)

Fuente: Elaboración propia a partir de las fuentes citadas.

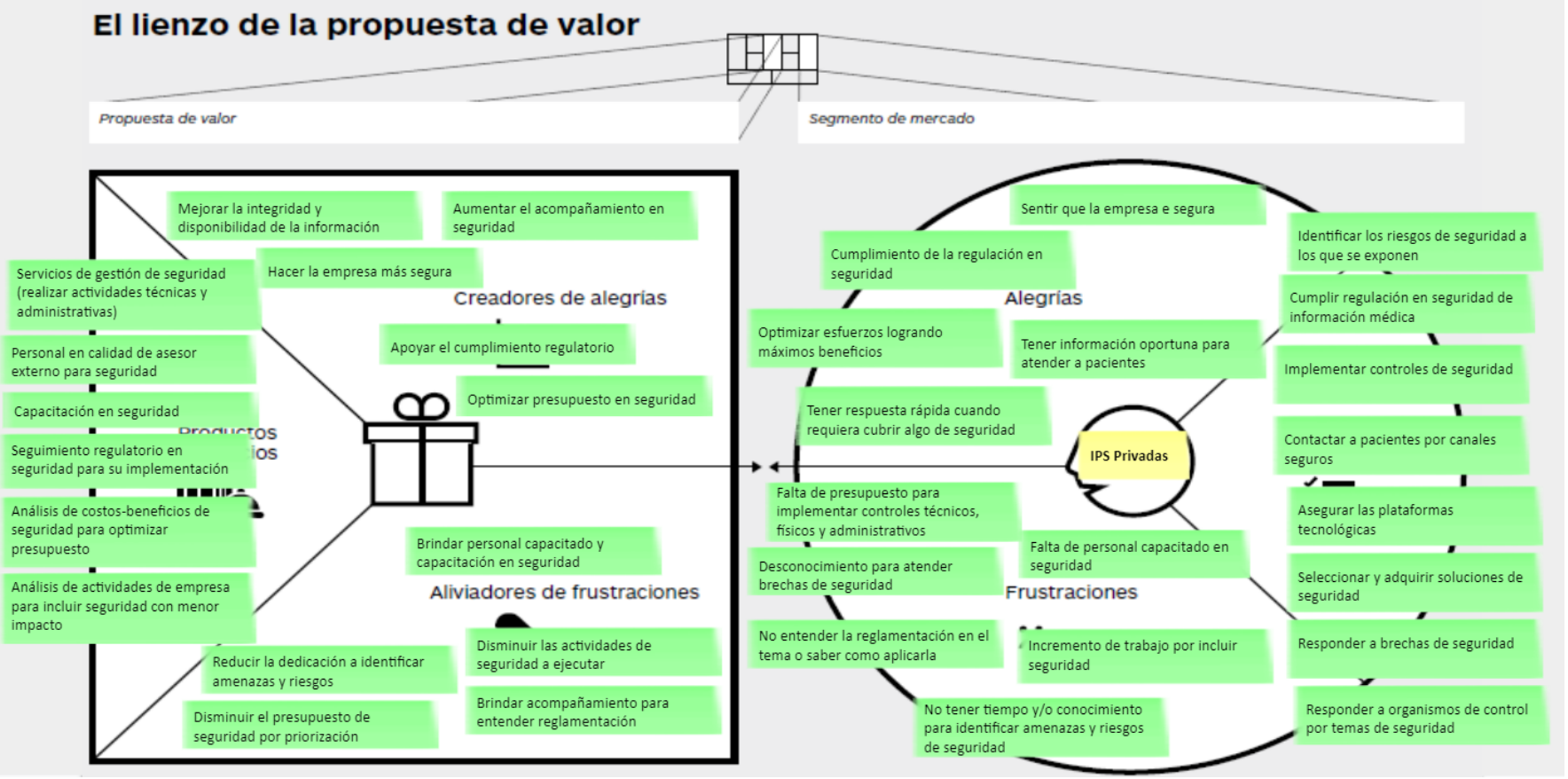
En las frustraciones, aunque las empresas son conscientes que temas como la creación de registros médicos electrónicos y la sistematización de estos son una ventaja para la operación y la prestación del servicio, se identifica que su uso abre la posibilidad a nuevas amenazas de seguridad, lo cual genera preocupación por la protección de la información y el cumplimiento normativo. De otra parte, aunque tener conciencia en seguridad para las IPS puede enmarcar la realización de varios de sus trabajos, el entrenamiento y capacitación a personal en temas de seguridad y privacidad no es un tema al que se le de relevancia, pero se considera una frustración a la hora de atender la protección de la información médica. Esto se debe en algunos casos a que simplemente no se considera necesario, no se cuenta con los recursos para realizar estas capacitaciones o contratar personal especializado en seguridad que cubra esta necesidad.

Respecto a las alegrías, una de las principales es el contar con información oportuna en el momento requerido (Åhlfeldt & Söderström, 2008) siempre y cuando se pueda lograr, lo que en algunas instituciones prestadoras de salud es complejo, por la ausencia de interoperabilidad entre empresas. Además, se consideran alegrías el cumplimiento regulatorio, considerar que la empresa se encuentra en un punto de seguridad, responder rápida y oportunamente a brechas de seguridad y establecer un Pareto 80/20 entre beneficio en seguridad sobre esfuerzo (Canadian Centre for Cybersecurity, 2021).

A partir de los trabajos, alegrías y frustraciones se definieron los generadores de alegrías, aliviadores de frustraciones y los productos y/o servicios que pueden cubrir estos. Esto

corresponde con el mapa presentado del lado izquierdo del lienzo de la propuesta de valor en la Figura 11. Los generadores de alegrías y los aliviadores de frustraciones tienen en cuenta cómo, a partir de acciones puntuales que se pueden brindar en la propuesta de valor, se puede dar cubrimiento a estos requerimientos considerando las limitaciones de las empresas de salud. La propuesta se enfoca en la tercerización de servicios de seguridad por parte de las IPS privadas como se presenta en el apartado siguiente.

Figura 11. Lienzo de la propuesta de valor



Fuente: Elaboración propia.

Propuesta de valor

Sågänger & Utbult (1998), como se citó en Söderström, Åhlfeldt, & Eriksson (2009), indicaron que el principal propósito de la seguridad de la información en el sector salud es lograr la seguridad y cuidado médico de los pacientes y la privacidad de sus datos. La seguridad hace referencia a proveer a los pacientes con oportunidades para el mejor cuidado personal, teniendo la información correcta (integridad) en el momento correcto (disponibilidad) y la privacidad de su información sensible para protegerla de distribución no autorizada (confidencialidad). Por esto es requerida una perspectiva orientada al proceso de prestación de servicios médicos que tome la seguridad de la información en consideración.

Con lo anterior, la propuesta de valor que propone este trabajo considera la inclusión de la seguridad de la información como parte del ADN de la cadena de valor de las instituciones prestadoras de servicios de salud, con lo cual esta no sea un elemento aislado, sino que sea parte de estas organizaciones. Para ello es necesario partir del análisis de los procesos y actividades de la institución, con el fin de identificar situaciones problema dónde se pueda ver afectada la integridad, disponibilidad y/o confidencialidad de la información médica. Lo anterior se refiere a realizar gestión de la seguridad por diseño, porque parte de analizar el diseño y operación de las actividades para prestar los servicios de salud y con ello incluir desde el mismo flujo de operación los componentes de seguridad.

De acuerdo con (Heikkilä, Bouwman, & Heikkilä, 2018) las Pymes pueden estar interesadas en innovar en sus modelos de negocio por dos esquemas: primero por rentabilidad, haciendo foco en el diseño o mejora de actividades clave y recursos; segundo, por crecimiento, por lo cual el foco se da a partir de la relación con los clientes, el conocimiento de estos y la mejora de la oferta. Crecimiento y rentabilidad hacen parte de los objetivos estratégicos de las Pymes.

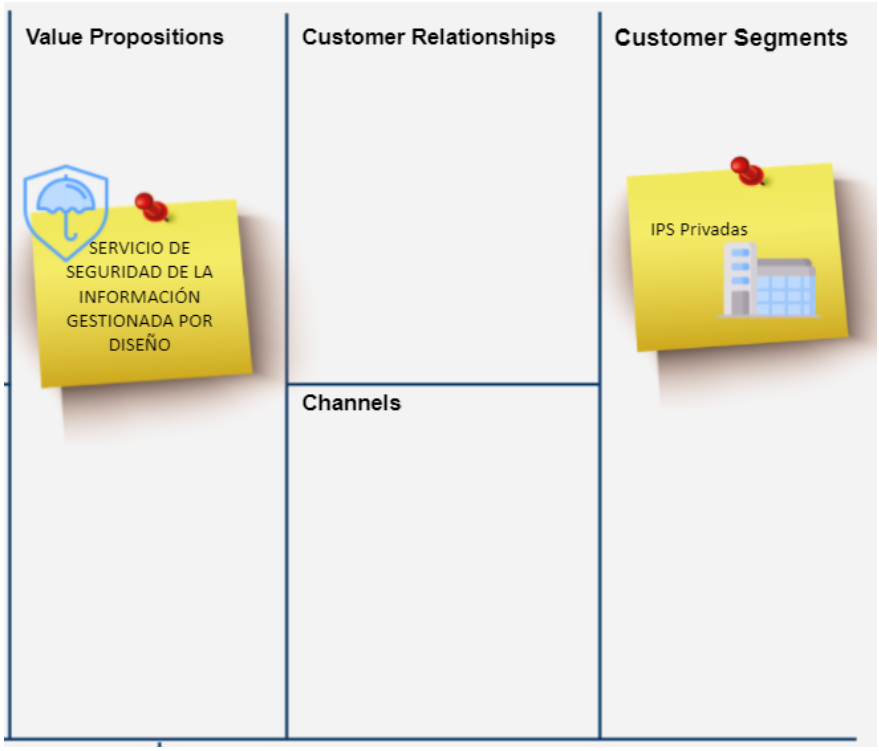
Las Pymes de salud no están exentas a estos elementos. Con los cambios en las necesidades del mercado, las empresas de salud han tenido que volcarse en mayor medida al uso de tecnología, convirtiéndose esta en un recurso clave en sus operaciones para la prestación del servicio y el contacto con los clientes. Esto ha llevado a la implementación de modelos y proyectos de *eHealth*[9]. Por ejemplo, ahora los profesionales independientes y las instituciones médicas están utilizando medios digitales como SMS para promover sus servicios, pero se puede prestar para suplantación de la entidad generando mala imagen para la empresa. Por ello es importante la inclusión de la seguridad desde la misma cadena de valor del negocio.

El concepto global bajo el cual se propone la propuesta de valor es un Servicio de Seguridad de la Información, gestionado por diseño y desde el cual se identifiquen riesgos de seguridad de la información a los que se encuentre expuesta la información médica, y a partir de ello desplegar las actividades que permitan mitigar estos riesgos en las instituciones para hacerlas más seguras. Para ello se contará con personal especializado en seguridad de la información, en calidad de asesor externo y que realice las siguientes actividades: 1) Analizar las actividades de la institución para incluir componentes de seguridad de la información con el menor impacto desde su flujo de operación, a partir de esto 2) analizar riesgos de seguridad de la información, 3) asesorar en la identificación y análisis de reglamentación y normativa en seguridad de la información que aplique a la institución, 4) definir, implementar y operar medidas de control para mitigar los riesgos identificados (actividades técnicas y administrativas) con un enfoque de optimización en costos - beneficios, 5) apoyar en la respuesta y gestión de eventos y/o incidentes de seguridad que puedan

[9] Uso de tecnologías de la información y la comunicación en los servicios de salud

presentarse, y 6) crear y mantener la documentación necesaria para soportar los servicios anteriores (Figura 12).

Figura 12. Propuesta de valor



Fuente: Elaboración propia.

Para la actividad cuatro se considera como línea base de controles a implementar los propuestos por (Paulsen & Toth, 2016; Canadian Centre for Cybersecurity, 2020; Da Silva, Dias, & Lira, 2015; Kissi, Baozhen, Clemency, & Amoah-Anomah, 2018; Armstrong, 2000; Fatima & Colomo-Palacios, 2018), que corresponden con una propuesta simplificada de seguridad para Pymes y controles propios de seguridad en salud: alineación de la seguridad con la organización y gobierno de seguridad, análisis de riesgos, antivirus, seguridad de Internet, seguridad de redes, seguridad de datos, parches de seguridad, *backups*, seguridad física, seguridad en *Wireless*,

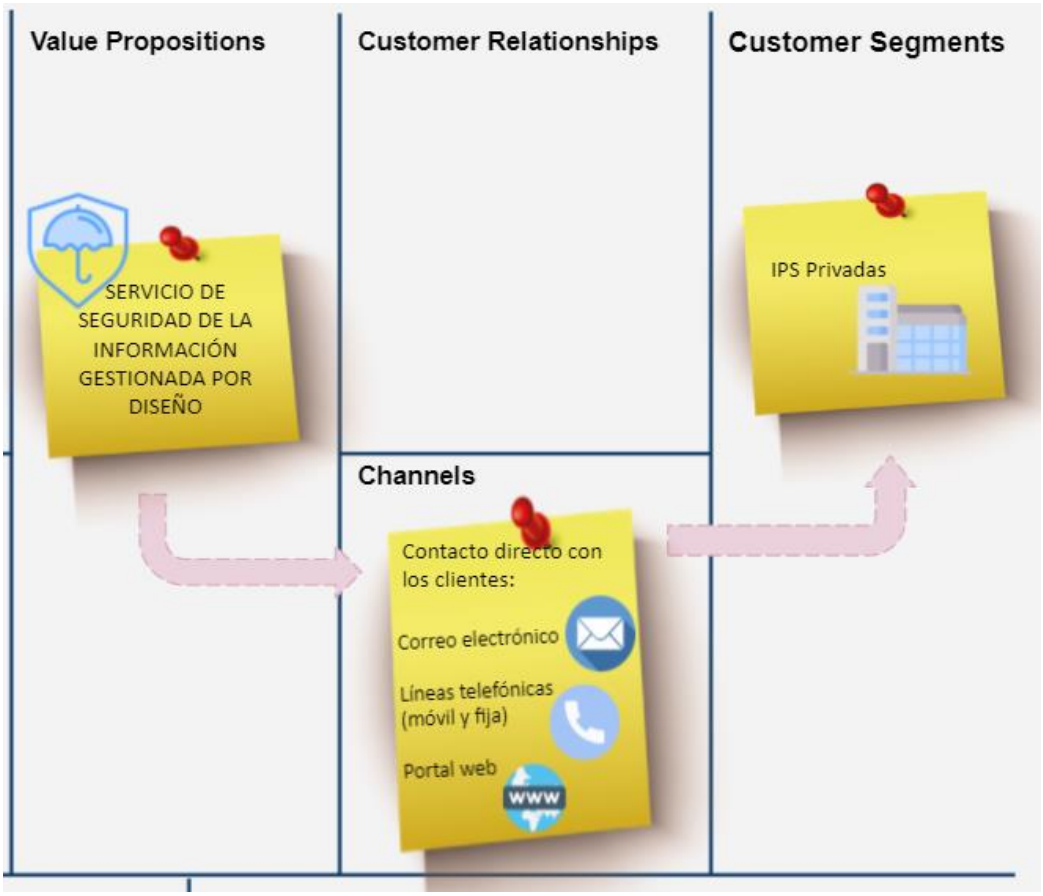
conciencia y entrenamiento de empleados, gestión de cuentas de usuario, implementar controles de accesos y gestionar cumplimiento regulatorio de seguridad.

Las actividades planteadas como parte de la propuesta consideran los trabajos del cliente, sus alegrías y frustraciones, los aliviadores de frustraciones y los creadores de alegrías identificados previamente. A continuación, se presentan los canales a través de los cuales se establece la comunicación con las IPS privadas.

Canales

Los canales a través de los cuales se contacta a la IPS privadas para llevar los servicios de la propuesta de valor son propios. Se definen como tipos de canales el portal web, correo electrónico y líneas telefónicas: celular y fija (Figura 13). A través del portal se brindará información general de la propuesta de valor y los servicios que la integran para que los clientes tengan oportunidad de conocerla e interesarse, estableciendo contacto para pedir información adicional. Con el correo electrónico y las líneas telefónicas, los clientes recibirán asesoría comercial y técnica como se indica en el siguiente apartado de relaciones con los clientes.

Figura 13. Canales



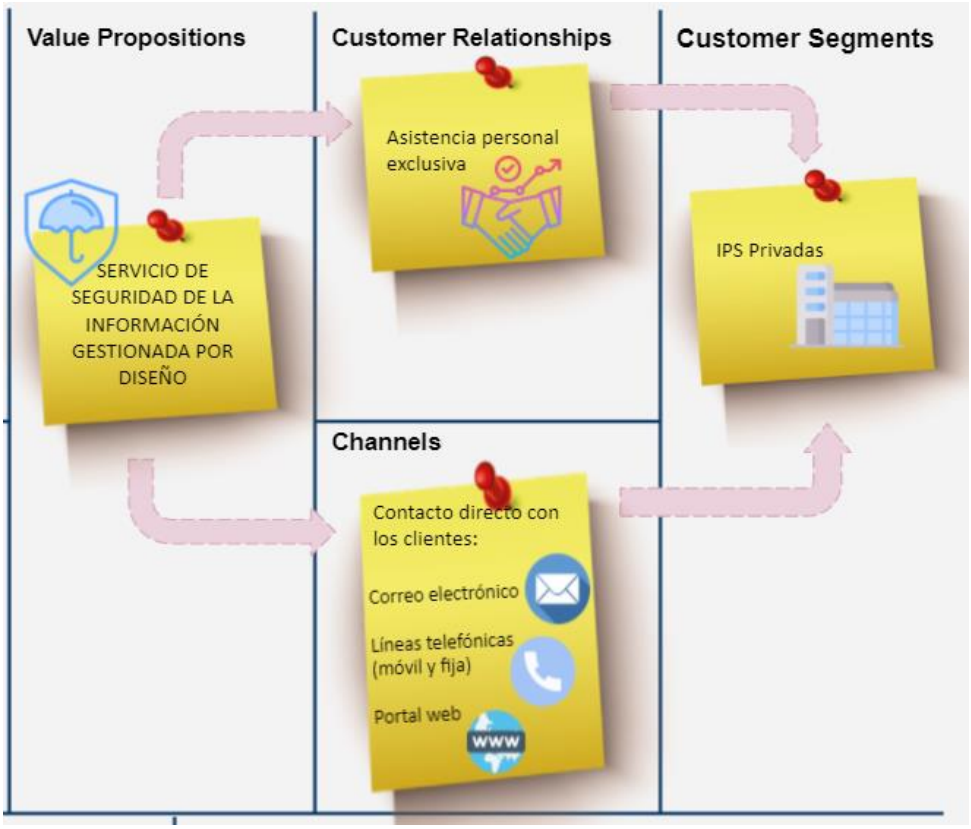
Fuente: Elaboración propia.

Relaciones con clientes

Las relaciones con los clientes se establecen bajo la categoría de asistencia personal exclusiva (Osterwalder & Pigneur, 2011) en la cual los clientes pueden comunicarse con representantes de servicio de atención al cliente bajo un esquema de dos vías: una orientada a mantener las relaciones comerciales con los clientes, y otra orientada a la asesoría técnica especializada en lo que respecta a la prestación propia de los servicios. El objetivo de realizar esta separación es mantener niveles adecuados de servicios respecto a temas administrativos como la facturación, el seguimiento a la satisfacción del cliente y sus necesidades de servicio y; de otra

parte, gestionar los requerimientos técnicos y de operación de los servicios de seguridad bajo condiciones de calidad. Para esto se considera contar con un equipo comercial y un equipo técnico (Figura 14).

Figura 14. Relaciones con clientes



Fuente: Elaboración propia.

En los dos casos el objetivo es fidelizar clientes a partir de que estos perciban un acompañamiento personalizado que ayude, de una parte a estimular la adquisición de nuevos servicios de seguridad de la información, que puedan ser requeridos y mantener los definidos en la propuesta; y de otra parte, generar relaciones de alianza que permitan que las IPS privadas, que sean clientes, refieran a otras empresas del sector salud los servicios que componen esta propuesta de valor y con esto capturar nuevos clientes.

Fuentes de ingresos

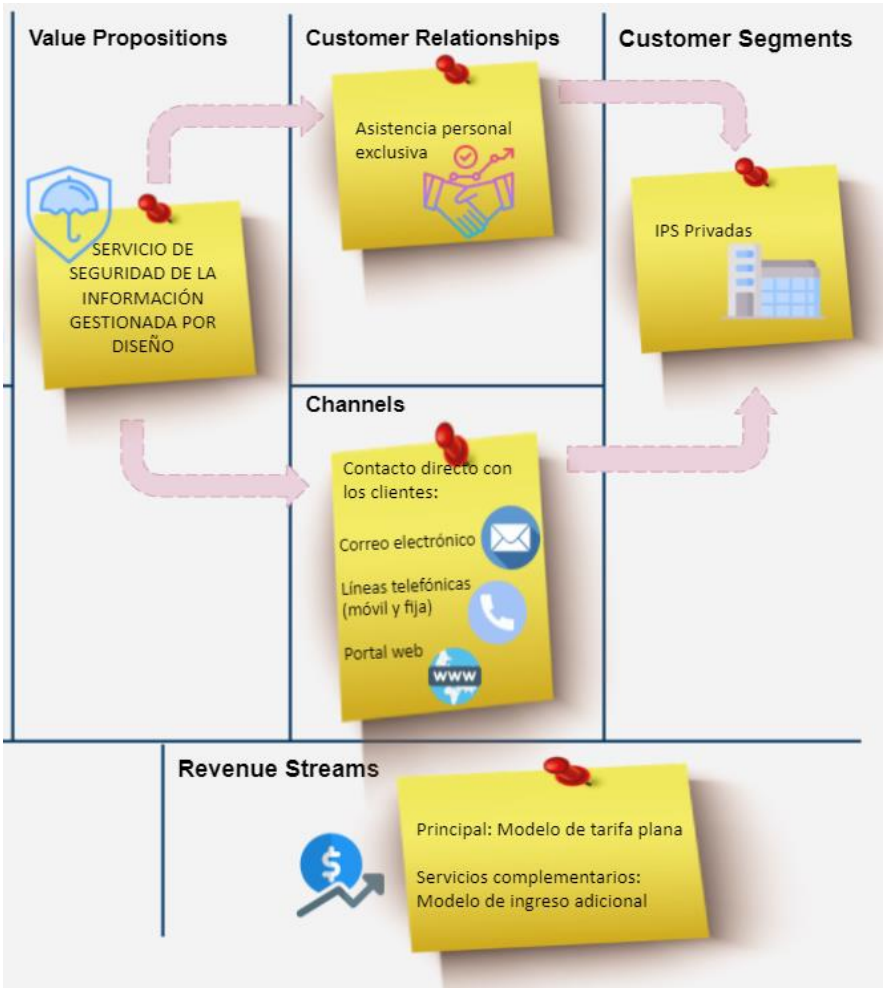
Para mantener la calidad de los servicios asociados en la propuesta de valor, es primordial contar con el personal técnico especializado que pueda atender los requerimientos de operación de los clientes. De igual forma, es necesario dar cubrimiento a los costos y gastos administrativos (gestión comercial, actividades financieras, nómina, gestión del talento humano, mercadeo, entre otros) y de operación (mantenimiento de infraestructura tecnológica, software y hardware requerido para la gestión de seguridad), por lo cual se hace necesario mantener un flujo de caja que permita el sostenimiento de la empresa de servicios.

Como lo indica Williams (2013), dado que las Pymes son diferentes de las grandes empresas en estructuras organizativas y en enfoques operativos, típicamente muestran atributos de falta de recursos y estilos de gestión no sistemáticos. Como resultado, las medidas de seguridad de la información a implementar son muy sensibles a los factores de costos y no necesariamente se provee la mejor cobertura, sino la cobertura asequible.

Para dar cubrimiento a esta necesidad se considera como fuente de ingresos principal un modelo de *tarifa plana* (Gassmann, Frankenberger, & Csik, 2014), a partir del cobro de una tarifa fija mensual con una variación, considerando opciones de contratos a términos de seis (6), doce (12), o veinticuatro (24) meses. A mayor sea el tiempo que se pacte el contrato con el cliente, el valor mensual de los servicios será menor, lo anterior para buscar generar economías al cliente y asegurar los ingresos fijos mensuales a la empresa como parte de su sostenimiento. La idea de este modelo es hacer la seguridad más accesible a las Pymes (Canadian Centre for Cybersecurity, 2020).

Sin embargo, pueden presentarse servicios complementarios que no se cubran dentro de la propuesta de valor y representen un ingreso adicional derivado por un pago puntual del cliente (por ejemplo, implementaciones tecnológicas o proyectos que surjan en la empresa y para los cuales requieran una asesoría diferenciadora). Esto representaría una fuente de ingresos complementaria que se manejaría bajo un modelo de *ingreso adicional* (Gassmann, Frankenberger, & Csik, 2014), como se presenta en la Figura 15.

Figura 15. Fuentes de ingreso



Fuente: Elaboración propia.

Adicionalmente se posibilita la negociación con los clientes para pactar el precio mensual, considerando para su definición el tamaño de la empresa, el número de empleados, la cantidad de sedes y la tecnología existente. Con esto se busca llegar a plantear una subdivisión dentro del segmento de clientes, solo con fines del modelo de ingresos, de forma tal que puedan establecerse precios diferenciados para ofrecer la propuesta de valor a empresas de menos recursos en un modelo de bajo costo y que se logre, a partir del valor adicional que paguen las empresas de mayores recursos, el equilibrio económico en la fuente de ingresos, esto corresponde a un modelo *Robin Hood* (Gassmann, Frankenberger, & Csik, 2014). Lo anterior dejando claro que, si bien se habla de una subdivisión, esta sigue estando dentro del alcance referido como IPS privadas.

Este planteamiento de fuentes de ingresos busca que las IPS privadas, siendo Pymes con recursos limitados, realicen actividades preventivas en seguridad que representen una menor inversión, en lugar de mantener su aproximación a un enfoque operativo con una respuesta reactiva a eventos de seguridad y el subsecuente reflejo en gastos (Williams, 2013).

Una vez definidos los elementos del modelo de negocios orientados hacia afuera en la relación con los clientes, a partir del siguiente módulo se definen los elementos requeridos hacia el interior de la empresa de servicios para lograr generar la propuesta de valor definida.

Recursos clave

En este apartado, se precisan los recursos tangibles e intangibles que permiten la entrega de la propuesta de valor y que permiten que el modelo de negocio funcione. Estos incluyen recursos humanos, físicos y organizacionales.

La seguridad en Pymes se limita respecto a empresas grandes (European Digital SME Alliance, 2019), estas últimas tienen mayores ventajas sobre las primeras respecto a niveles más

profundos de especialización, mayor ventaja de conocimiento en ciencia, capacidad para aprovechar economías de escala, acceso a recursos financieros más baratos y grandes, y mejor gestión de riesgos (Okundaye, Fan, & Dwyer, 2019), así como han madurado en sus inversiones para proteger la información, incluyendo tecnología, personas, procesos y presupuesto para mejorar la solidez en seguridad. Las Pymes no tienen estos recursos equivalentes para construir un marco de seguridad sólido (Alshboul & Streff, 2015).

En relación con el personal, la probabilidad de que una Pyme tenga un número grande de personal dedicado a tecnología altamente calificado es baja, e incluso es muy poco probable que tenga personal en el área de tecnología dedicado a seguridad de la información; teniendo en cuenta la cantidad de empleados en Pymes respecto a grandes empresas (entre 11 y 200 empleados en Pymes para el caso de Colombia) (Williams, 2013).

De acuerdo con una investigación realizada por Dimopoulos, Furnell, Jennex & Kritharas (2004) en una encuesta practicada a Pymes de Europa y Estados Unidos (121 Pymes en total) se identificó que en un 50% de los casos, el responsable de seguridad es el administrador de TI. Solo el 9% de las medianas empresas cuenta con una persona específica dedicada a seguridad, lo cual representa un 2,5% del total y el 47,5% de la totalidad de empresas tienen delegada esta responsabilidad en otro cargo que puede no contar con el conocimiento y la experiencia para estas actividades.

En el caso colombiano, de acuerdo con la Gran Encuesta TIC realizada en 2017 (Luna, 2017) el 57,3% de las medianas empresas y el 63,1% de las pequeñas indicaron que no cuentan con personal de TI debido a que el negocio no lo exige, o que es muy costoso tenerlo (23% y 15,5% respectivamente), por lo cual para estas empresas (234 Pymes) tener un área, cargo o rol

dedicado a la seguridad de la información ni siquiera es un aspecto por considerar. En la Tabla 21 se presentan los datos obtenidos de carencia de personal dedicado a tecnología y seguridad en pequeñas y medianas empresas colombianas.

Tabla 21. Pymes sin personal dedicado a tecnología y seguridad

Tamaños empresa	**Colombia**	
	Carece de personal de TI	**Carece de personal de seguridad**
Medianas	30,7%	52,9%
Pequeñas	49,4%	68,6%

Fuente: Adaptado de Luna (2017) Tabla anexa (Excel) al estudio con datos ponderados

Respecto a tecnología, se presenta una escasa inversión en esta y en herramientas (*software* y *hardware*) específicas de seguridad de la información (Dimopoulos, Furnell, Jennex, & Kritharas, 2004). En un estudio realizado en Nigeria por Okundaye, Fan & Dwyer (2019) sobre el impacto de las tecnologías en las Pymes, identificaron que el consenso estaba de acuerdo en que los costos financieros de implementar tecnologías de la información, particularmente en Pymes, es un significante factor que debe ser considerado antes de decidir la adopción de tecnología. La inversión inicial en TI es restrictiva dado que apenas pueden permitirse el costo de operación diario. El costo de compra de *software* y equipos, contratar personal calificado en TI, y capacitar al personal existente, así como otros costos asociados con adopción de TI, está prohibido para muchos pequeños negocios.

No obstante, hay empresas que reconocen la importancia de la inversión en tecnología para su operación y los beneficios de esta; el problema radica en implementar tecnología que soporte procesos de negocio sin las herramientas de seguridad necesarias y adecuadas para asegurar las

operaciones digitales o electrónicas que se realizan al utilizar esta, lo cual puede verse reflejado en brechas de seguridad. Por ejemplo, en una encuesta realizada por Subramoniam & Sadi (2010) sobre el concepto de la web 2.0 en la salud en Estados Unidos para el año 2009, identificaron que el 60% de los encuestados solo gastan el 3% de su presupuesto de tecnología para seguridad. De forma similar, por una encuesta realizada a Pymes en relación con prácticas de seguridad (Prince & King, 2012) en Reino Unido se identificó que la priorización de presupuesto de tecnología no se traslada a presupuesto en seguridad, dado que cerca del 47% de los encuestados respondieron que gastan menos del 5% de su presupuesto de TI en seguridad.

Respecto a los procesos, en una encuesta realizada para Pymes por la Universidad de Lancaster en Reino Unido (Prince & King, 2012), el 98% de los encuestados respondió que la seguridad es una prioridad alta para el negocio, sin embargo, solo el 43% contaba con una política de seguridad documentada. De forma específica en el sector salud, en un estudio realizado en Estados Unidos respecto al cumplimiento de la ley HIPAA, se identificó que un gran número de centros médicos no cuentan con políticas y procedimiento de seguridad (Chen & Benusa, 2017).

A partir del análisis de los datos anteriores, en la Tabla 22 se presentan los recursos clave identificados para generar y entregar la propuesta de valor.

Tabla 22. Recursos clave

Tipo de recurso	**Descripción**
Humanos	Personal técnico especializado: Personal con conocimientos específicos en seguridad de la información y esquemas de operación del sector salud para brindar los servicios profesionales de seguridad. Se contará con personal de nómina, así como aliados especializados que, bajo esquema de prestación de servicios o contrato obra labor, sean los encargados de prestar el servicio.

	Personal comercial: Personal del área comercial para la asistencia personal exclusiva brindada a las IPS privadas en lo concerniente a aspectos administrativos del servicio.
Físicos	Infraestructura tecnológica (*hardware* y *software* con propósito específico en seguridad de la información) que es requerido para brindar los servicios al cliente. Puede requerirse software y hardware particular para algún cliente, según el análisis que se realicen de sus necesidades de seguridad, pero a priori para todas las IPS privadas se considera: *antimalware*[10], *firewall*[11], directorio activo, herramienta de inventarios de *software* y *hardware*, solución de *backups*[12] de información.
Organizacionales	Conocimiento y experticia técnica para la prestación de servicios (*Know how en seguridad aplicado al sector salud y adaptado a las IPS privadas*) por ejemplo, aquí se considera la generación de procedimientos y documentos guía específicos para aplicar seguridad en estas empresas. Bases de datos de aliados y proveedores que permiten llevar la propuesta de valor con mejores costos en lo que respecta a la adquisición y/o alquiler del *software* y *hardware* mencionado.

Fuente: Elaboración propia.

El recurso humano es el más importante para el modelo de negocio, al tratarse de una propuesta basada en servicios, donde se requiere un alto nivel de conocimiento especializado.

Actividades clave

Las actividades clave representan las acciones de mayor importancia que deben ser realizadas para que la propuesta de valor pueda ser entregada a los clientes. Dado que la propuesta de valor se enfoca en servicios e implica un alto nivel de conocimiento e intelecto que recae en el personal, las actividades de atracción, capacitación y retención del personal técnico son críticas, puesto que es necesario generar confianza en el cliente frente a la preparación del personal que lo

[10] Software especializado para detectar y eliminar los programas maliciosos
[11] Hardware o software diseñado para bloquear accesos no autorizados y permitir comunicaciones autorizadas
[12] Respaldo o copia de reserva de la información

atienda, así como mantener el conocimiento de la atención prestada mientras se mantenga el servicio a un determinado cliente. Al ser la propuesta de valor enfocada en precios bajos, el equipo técnico se apalancará principalmente en asociaciones clave con especialistas independientes en seguridad y tecnología, con lo cual se reduzcan los costos asociados a nómina y se manejen esquemas de contratos obra labor o prestación de servicio.

A partir de contar con este personal se realizan las siguientes actividades clave que hacen parte integral de la propuesta de valor: 1) Analizar las actividades de la IPS privada para incluir componentes de seguridad de la información con el menor impacto desde su flujo de operación durante la vigencia del servicio, 2) analizar riesgos de seguridad de la información de las actividades de la institución, 3) asesorar en la identificación y análisis de reglamentación y normativa en seguridad de la información que aplique a la IPS privada, 4) definir, implementar y operar medidas de control para mitigar los riesgos identificados (incluida la operación de la infraestructura tecnológica de seguridad del cliente) con un enfoque de optimización en costos - beneficios, 5) capacitar al personal de la IPS en seguridad de la información, 6) apoyar en la respuesta y gestión de eventos y/o incidentes de seguridad que puedan presentarse, y 7) crear y mantener la documentación necesaria para soportar los servicios anteriores. En la Figura 16 se presentan las actividades clave descritas.

Figura 16. Actividades clave

Fuente: Elaboración propia.

Asociaciones clave

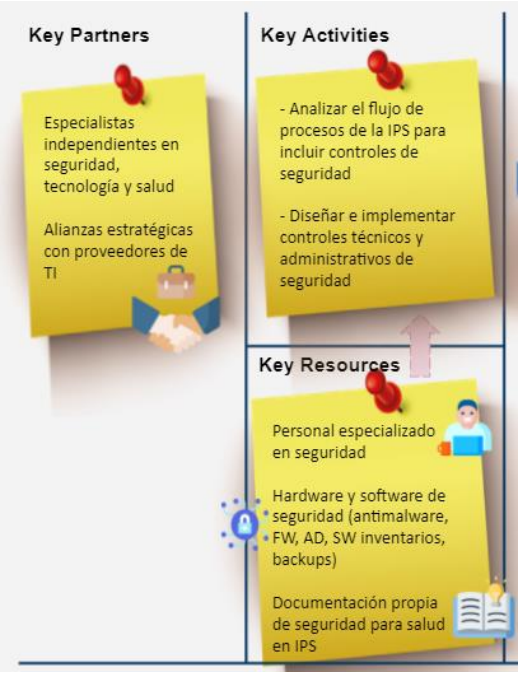
Para lograr generar un modelo de negocio con una propuesta de valor de bajo costo a los clientes, es necesario establecer asociaciones clave con proveedores de servicios tecnológicos (*hardware*, *software* y servicios de TI) que permitan obtener economías de escala, cuyo beneficio se traslade al cliente al compartir recursos como infraestructura tecnológica y componentes de seguridad de la información. Las soluciones tecnológicas que son requeridas en primera instancia son: *antimalware*, *firewall*, directorio activo, herramienta de inventarios de *software* y *hardware y* solución de *backups* de información, que la empresa de servicios no tiene y se necesitan para cumplir la propuesta de valor. Para esto las asociaciones clave permitirían obtener dichas soluciones de *software* y *hardware* a precios más asequibles, puesto que se buscaría que su adquisición o alquiler se realizara bajo un modelo de economía en escala, que sería dirigido a

varias IPS privadas como clientes, es decir, algunos recursos serían compartidos considerando todas las medidas de separación por configuraciones requeridas para permitir que sean seguras.

Adicional, como parte de las asociaciones clave se considera la alianza con empresas que ofrezcan servicios de tecnología, con las cuales se puedan realizar colaboraciones en lo que respecta al soporte de infraestructura tecnológica de los clientes.

Por último, se considera asociaciones clave con especialistas independientes en seguridad, tecnología y servicios de salud a los cuales se recurrirá para operar y atender temas técnicos dado su conocimiento experto para soportar los servicios prestados a los clientes y a los cuales se pueda contratar como asesores en la modalidad de prestación de servicios u obra labor, esto con el fin de no impactar los costos operativos. La Figura 17 presenta las asociaciones clave.

Figura 17. Asociaciones clave

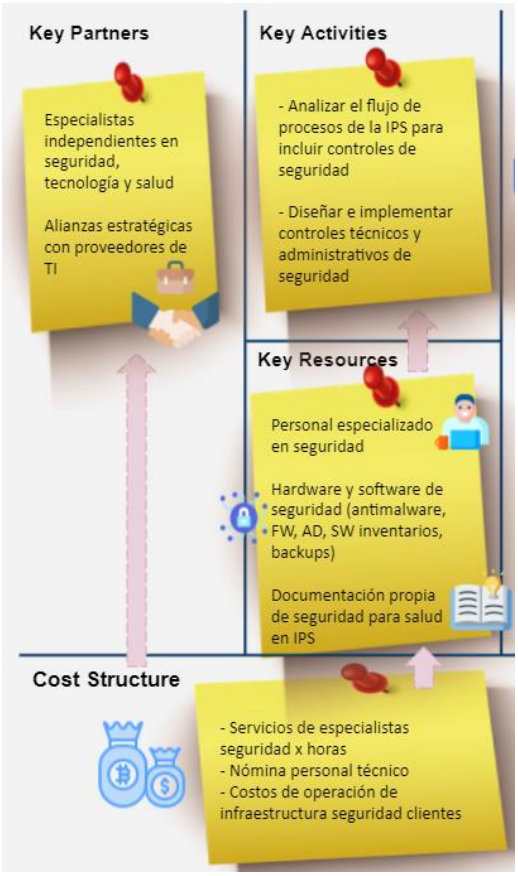


Fuente: Elaboración propia.

Estructura de costos

El módulo final del Canvas considera la estructura de costos requerida para entregar la propuesta de valor. Aquí se relacionan los costos y gastos necesarios para la creación y entrega de valor, así como para operar y mantener la propuesta. Dado que unos de los objetivos de la propuesta de valor es lograr que sea de bajo costo, esta estructura se basa en recortar los gastos donde sea posible maximizando el uso de los recursos. A esto se hacía referencia cuando se planteaba la importancia de trabajar con especialistas independientes en seguridad y tecnología, así como lograr asociaciones clave para obtener beneficios por economías de escala en infraestructura tecnológica y servicios de seguridad y TI. En la Figura 18 se presentan los principales costos y gastos a considerar.

Figura 18. Estructura de costos

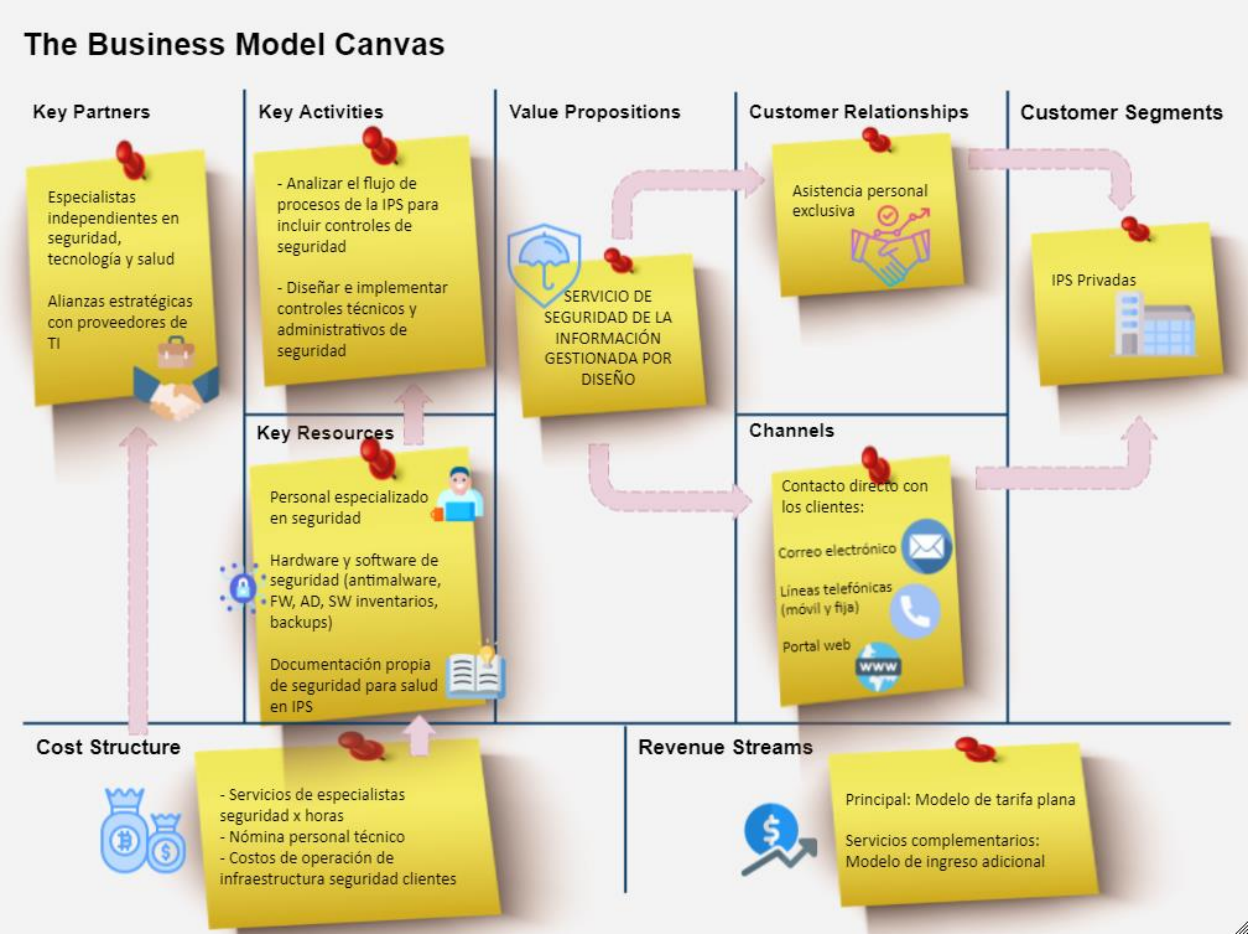


Fuente: Elaboración propia.

Sin embargo, algunos costos fijos se requieren mantener como los asociados a servicios (Internet, servicios de telefonía, mantenimiento del portal web, servicios de ofimática básicos) que hacen parte de los requerimientos de operación para atender al cliente.

A partir de lo anterior se cuenta con el modelo de negocio propuesto para prestar servicios de seguridad de la información a las IPS privadas que fueron seleccionadas como segmento de mercado. El modelo completo se presenta en la Figura 19.

Figura 19. Canvas servicios de seguridad de la información para IPS privadas



Fuente: Elaboración propia.

Este modelo de negocio busca brindar los elementos base que permitan la implementación de la seguridad de la información en las IPS privadas del sector salud. Su base considera las limitaciones en recursos económicos con las que cuentan estas empresas, por lo que considera que adquieran servicios de seguridad sin la necesidad de incrementar su planta de personal interna y se basa en el análisis propio de la cadena de valor de la empresa para implementar actividades de seguridad en los puntos que sea necesario. De forma adicional considera el acompañamiento constaste a los empresarios del sector para asistirlos y asesorarlos en los conceptos de seguridad y privacidad, partiendo de un análisis de los riesgos a los cuales pueden verse expuestas sus empresas, infraestructura y la información médica que manejan.

Conclusiones y trabajos futuros

Los riesgos de seguridad y privacidad de la información médica actualmente cuentan con mayor reconocimiento. La necesidad de proteger la información se afianza desde los gobiernos que están definiendo normativas que exijan a las empresas la implementación de controles para su protección. En el caso colombiano, en la medida en que la regulación frente a seguridad de datos personales pueda llegar a ser más fuerte, es posible que aumente los requerimientos de personal especializado en seguridad para apoyar los procesos de implementación técnica con los que las Pymes logren cumplimiento, como sucedió en Estados Unidos cuando se aprobó la ley HIPAA. De por sí, es necesario que se creen estándares y reglamentación específica para seguridad de la información en el sector salud en el país. El camino aún es largo, puesto que es necesario reforzar en la cultura organizacional y social la necesidad de proteger estos datos, así como brindar a micro, pequeñas y medianas empresas elementos con los cuales facilitarles la labor en esta carrera por la protección de la información.

La metodología empleada permitió cumplir con el objetivo de diseñar un modelo de negocio de servicios de seguridad de la información para las Pymes del sector salud en Bogotá, contando con el análisis del contexto en el cual están estas empresas, los riesgos, oportunidades, necesidades y limitaciones asociados a partir de la revisión en profundidad de 46 documentos resultantes luego de realizar un filtro de 704 textos relacionados con seguridad de la información en Pymes del sector salud e información de modelos de negocio enfocados en seguridad y salud. A partir de esto se identificó el segmento específico de mercado al cual se puede ofrecer la propuesta de valor, los elementos base que debe contener esta a partir de los trabajos, alegrías y frustraciones de estos clientes frente a seguridad de la información, y con ello los canales de comunicaciones y relaciones clave para entregar la propuesta al cliente, considerando un modelo

de ingresos que busca ser costo eficiente para las Pymes de salud, sin dejar de lado los requerimientos de ingresos y rentabilidad para la empresa de servicios, con lo cual se pueda dar su sostenimiento en el tiempo.

Una vez realizado esto, se identificaron las actividades, recursos y asociaciones claves que al interior de la empresa de servicios permitan entregar la propuesta de valor, mantenimiento y control sobre los costos y los gastos, a fin de optimizar los recursos sin perder de vista el cumplimiento de las necesidades de los clientes y los requerimientos de calidad en la gestión de servicios.

Con la investigación de herramientas, metodologías y ontologías para el desarrollo de modelos de negocio se reconocieron propuestas de diferentes autores para la generación de estos y con ello determinar que el Canvas como herramienta para la generación de modelos de negocio permite en su narrativa la construcción del modelo, considerando cada uno de los pasos requeridos para crear valor para el cliente y elegir elementos adecuados que permitan entregarlo y capturarlo.

Trabajos futuros

El sector de servicios de salud continuará evolucionando como respuesta a los desafíos actuales para dar cubrimiento a usuarios y pacientes, al igual que continuará prestando servicios ante situaciones como los requerimientos de distanciamiento social por eventos como la pandemia por el COVID-19 o las limitaciones por el acceso a servicios médicos en lugares alejados de las grandes ciudades. En este sentido, el aumento en el uso de aplicaciones y tecnología con propósito médico y sanitario seguirá en incremento y representará mayores avances en la industria de la salud (Gomes & Moqaddemerad, 2016) con el uso de dispositivos móviles (*mhealth*) y *wearables* orientados a salud, así como los modelos de negocio de salud se están orientando a servicios

digitales (telemedicina). En aplicaciones, dispositivos y servicios de este tipo han sido identificadas fallas de seguridad que pueden dejar expuestos datos médicos de las personas, con lo cual las posibilidades de investigación e inclusión de seguridad para estos es un campo de acción presente y futuro.

Además existen servicios específicos como *Kanta* (Kanta, s.f.) en Finlandia y *MyData* (MyData, s.f) en Europa, donde los ciudadanos y proveedores de servicios de salud cuentan con repositorios de registros médicos que pueden ser usados desde los requerimientos propios de cada uno y buscan temas de transparencia en el uso de información médica. Aunque al momento este tipo de servicios no ha llegado a Colombia, como ha pasado con otros elementos, llegará el momento en que se use en el país e implicará otro campo de investigación para la inclusión de medidas de seguridad en estos servicios, considerando el momento en que se utilice, la información que se considere incluir y las implicaciones de seguridad a partir de los esquemas usados para su implementación.

Por último, a partir de la reglamentación sobre historia clínica electrónica en el país del 2020, se presentarán desafíos respecto a las implementaciones técnicas que realicen las empresas de salud en los diferentes niveles de la cadena de funcionamiento del servicio para el manejo de la información médica y su protección en el intercambio que realicen entre entidades. Esto también representará un campo de acción desde la seguridad de la información y los esquemas de prestación de servicios que puedan ser ofrecidos a estas entidades desde la perspectiva de propuestas de valor.

Anexo 1. Textos tomados en la revisión de literatura

Título	Autor(es)	Año de publicación	Fuente de publicación
Impact of information and communication technology in Nigerian small-to medium-sized enterprises.	Okundaye, Kessington; Fan, Susan K.; Dwyer, Rocky J.	2019	*Journal of Economics, Finance & Administrative Science.*
Innovation capacities of Serbian small and medium-sized enterprises.	Stanković, Ljiljana, Djukić, Suzana, Lepojević, Vinko	2014	TEME: Casopis za Društvene Nauke
Reliance on Cryptography of Cloud Computing in Healthcare Information Management, Lessons for Ghana Health Service.	Kissi, Jonathan, Baozhen Dai, Clemency, Benedicta A., Amoah-Anomah, Grace	2018	*International Journal of Information Security Science*
Creación de una empresa de servicios de Seguridad Informática para sitios webs, orientada a PYMES dentro de la ciudad de Guayaquil.	Zambrano, Pablo Víctor	2015	Universidad Católica de Santiago de Guayaquil
From strategic goals to business model innovation paths: an exploratory study	Heikkilä, Marikka; Bouwman, Harry; Heikkilä, Jukka	2018	*Journal of Small Business and Enterprise Development*
HIPAA security compliance challenges: The case for small healthcare providers.	Chen, Jim Q., Benusa, Allen	2017	*International Journal of Healthcare Management*
Futures Business Models for an IoT Enabled Healthcare Sector: A Causal Layered Analysis Perspective.	Gomes, Julius Francis, Moqaddemerad, Sara	2016	*Journal of Business Models*
Value Creation in International Business: Volume 2: An SME Perspective	Svetla, Marinova; Jorma, Larimo; Niina, Nummela	2016	Value Creation in International Business

The ISACA Business Model for Information Security: An Integrative and Innovative Approach.	Von Roessing, Rolf	2010	Isse 2009 Securing Electronic Business Processes
Information security practices followed in the Indian software services industry: An exploratory study	Bahl, S.; Wali, O.P.; Kumaraguru, P.	2011	2011 Second Worldwide Cybersecurity Summit (WCS) Cybersecurity Summit (WCS)
Understanding the low-cost business model in healthcare service provision: A comparative case study in Italy	Cicellin, Mariavittoria; Adriana Scuotto; Canonico, Paolo; Consiglio, Stefano;Mercurio, Lorenzo	2019	Social Science & Medicine
How social business innovates health care: two cases of social value creation leading to high-quality services	Bohnet-Joschko, S.; Zippel, C.; Nelson, E.C.; Morgan, T.S.; Øvretveit, J.	2019	*Journal of Public Health* (Germany)
Healthcare 2.0	Subramoniam, Suresh; Sadi, Saifullah	2010	IT Professional IT Prof.
Future strategic topics in the business model of hospitals in Austria	Kriegel, J.; Riedl, A.; Tuttle-Weidinger, L.; Stöbich, A.-M.	2020	International Journal of Healthcare Management
A framework for information and communication technology induced transformation of the healthcare business model in Slovenia	Stanimirovic, D.	2015	*Journal of Global Information Technology Management.*
Investigating on requirements for business model representations: The case of information technology in healthcare	Gand, K.	2017	2017 IEEE 19th Conference on Business Informatics (CBI)
Applying the Australian and New Zealand Risk Management Standard to	Davidson, Robyn; Lambert, Susan	2004	*Australasian Journal of Information Systems*

Information Systems in SMES			
Literature Review of Information Security Practice Survey Reports	Yaping, Yang	2018	Jyväskylä: University of Jyväskylä
Small Business: Cyber Security Survey 2012	Prince, Daniel; King Nick	2012	Lancaster University
Effective Cyber Security Strategies for Small Businesses	Cook, Kimberly	2017	Walden University
Cyber-Security Policy Decisions in Small Businesses	Patterson, Joanna	2017	Walden University
Information security and privacy in healthcare: current state of research	Ajit Appari; M. Eric Johnson	2010	InderScience Online
Managing Information Security in Healthcare — an Action Research Experience	Armstrong, Helen	2000	SpringerLink IFIP International Information Security Conference - SEC 2000: Information Security for Global Information Infrastructures
A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment	Noor Hafizah Hassan; Zuraini Ismail	2012	*ScienceDirect*
Standards for information security and processes in healthcare	Eva Söderström; Rose-Mharie Åhlfeldt; Nomie Eriksson	2009	*Emerald Insight*
Managing Information Security in Healthcare: A Case Study in Region Skåne	Wallin, Emil; Xu, Ying	2008	Lund University School of Economics and Management
Managing Information Security and Privacy in Healthcare Data Mining	Cooper, Ted; Collman, Jeff	2005	*Springer Science*

Security aspects in healthcare information systems: A systematic mapping	Fatima, Aqsa; Colomo-Palacios, Ricardo	2018	*ScienceDirect*
Information Security Problems and Needs in Healthcare — A Case Study of Norway and Finland vs Sweden (Book Enterprise Interoperability III)	Åhlfeldt, Rose-Mharie; Söderström, Eva	2008	Springer
Information Security in Healthcare Sector	Narayana, Tvs; Naik, Naveen; Venkataiah, E.	2013	*International Refereed Journal of Engineering and Science* (IRJES)
Security and privacy in electronic health records: A systematic literature review	Fernández Alemán, José Luis; Carrión Señor, Inmaculada; Oliver Lozoya, Pedro Ángel; Toval, Ambrosio	2013	*ScienceDirect*
Security Control Requirements for Electronic Health Records	Abila, James Onyango; Kemboi, Lucy; Ronoh, Lamek	2019	*International Journal of Innovative Science and Research Technology*
Information Security Management of Healthcare System	Mahmood, Ashrafullah Khalid	2010	DiVA - Digitala Vetenskapliga Arkivet
A Maturity Model for Information Security Management in Small and Medium-Sized. Moroccan Enterprises: An Empirical Investigation	Matrane, Ossama; Talea, Mohamed	2014	*International Journal of Advanced Research in Computer Science*
A Strategic Model for Information Security Growth in Small and Medium Enterprises	Williams, Neville I	2013	Researchgate
Analyzing Information Security Model for Small-Medium Sized Businesses	Alshboul, Yazan; Streff, Kevin	2015	Americas Conference on Information Systems

Approaches to IT Security in Small and Medium Enterprises	Dimopoulos, Vassilis; Furnell, Steven; Jennex, Murray E.; Kritharas, Ioannis	2004	*Researchgate*
Information security and privacy standards for SMEs Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises	Galan Manso, Clara (ENISA); Rekleitis, Evangelos (ENISA); Papazafeiropoulos, Fotis (EY); Maritsas, Vasilios (EY).	2015	ENISA
Small Business Information Security: The Fundamentals NISTIR 7621 Revision 1	Paulsen, Celia; Toth, Patricia	2016	NIST
The EU Cybersecurity Act and the role of standards for SMEs	European Digital SME Alliance	2020	European Digital SME Alliance
Skills for SMEs - Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises	European Digital SME Alliance	2019	European Digital SME Alliance
Baseline Cyber Security Controls for Small and Medium Organizations V1.2	Canadian Centre for Cybersecurity	2020	Canadian Centre for Cybersecurity
Proposal for Simplified Security Model for Small and Medium Business	Da Silva Neto, Gonçalo Manoel; Dias Alencar, Gliner; Lira Queiroz, Anderson Apolonio	2015	XI Brazilian Symposium on Information Systems
Health care industry cybersecurity task force – Report on improving cybersecurity in the health care industry	Public Health Emergency	2017	Public Health Emergency
The Business Model for Information Security	ISACA	2010	ISACA

2019 HIMSS Cybersecurity survey	Healthcare Information and Management Systems Society	2019	Healthcare Information and Management Systems Society

Fuente: Elaboración propia.

Referencias

Abila, J., Kemboi, L., & Ronoh, L. (2019). Security Control Requirements for Electronic Health Records. *International Journal of Innovative Science and Research Technology, 4*(10), 137-141.

Afuah, A. (2004). *Business models: A strategic management approach.* New York: McGraw-Hill.

Afuah, A., & Tucci, C. L. (2001). *Internet Business Models and Strategies: Text and Cases* (2nd ed ed.). Mc Graw Hill. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/50617278/Internet_business_models_and_strategies_20161129-12210-7dd0bv.pdf?1480442808=&response-content-disposition=inline%3B+filename%3DInternet_business_models_and_strategies.pdf&Expires=1618031313&Signature=Zzm7Bxh

Åhlfeldt, R. M. (2008). Information Security in Distributed Healthcare - Exploring the Needs for Achieving Patient Safety and Patient Privacy. *Researchgate*. Obtenido de Researchgate: https://www.researchgate.net/publication/234059370_Information_Security_in_Distributed_Healthcare_-_Exploring_the_Needs_for_Achieving_Patient_Safety_and_Patient_Privacy

Åhlfeldt, R.-M., & Söderström, E. (2008). Information Security Problems and Needs in Healthcare — A Case Study of Norway and Finland vs Sweden. En K. Mertind, R. Ruggaber, K. Popplewell, & X. Xu, *Book Enterprise Interoperability III* (págs. 41-53). Skövde: Springer.

Alshboul, Y., & Streff, K. (2015). Analyzing Information Security Model for Small-Medium Sized Businesses. *Americas Conference on Information Systems,* 1-9.

América economía. (25 de 10 de 2019). *Ranking de clínicas y hospitales: estos son los mejores de Latinoamerica 2019*. Obtenido de América Economía - Cluster salud: https://clustersalud.americaeconomia.com/gestion-hospitalaria/ranking-de-clinicas-y-hospitales-estos-son-los-mejores-de-latinoamerica-2019

Amit, R., & Zott, C. (2001). Value Creation in E-Business. *Strategic Management Journal, 22*, 493-520. doi:10.1002/smj.187

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *InderScience Online*, 1-36.

Applegate, L. M. (2000). E-Business Models: Making Sense of the Internet Business Landscape. En G. W. Dickson, & G. DeSanctis, *Information Technology and the New Enterprise: Future Models for Managers* (págs. 49-94).

Armstrong, H. (2000). Managing Information Security in Healthcare — an Action Research Experience. *SpringerLink IFIP International Information Security Conference - SEC 2000: Information Security for Global Information Infrastructures*, 19-28.

Ascentor. (s.f.). *Cyber security myths putting SMEs at risk*. Obtenido de Ascentor: https://insights.ascentor.co.uk/blog/2020/10/cyber-security-myths-putting-smes-at-risk

Ashrafullah Khalid, M. (2010). Information Security Management of Healthcare System (Tesis). *Information Security Management of Healthcare System*. Karlshamn, Karlshamn, Suecia: DiVA - Digitala Vetenskapliga Arkivet.

AT&T. (s.f.). *Cybersecurity: A Problem Too Big for Small Business to Ignore*. Obtenido de Cybersecurity: A Problem Too Big for Small Business to Ignore: https://www.theatlantic.com/sponsored/att/cybersecurity-big-problem-for-small-business/1148/

Baden-Fuller, C., & Morgan, M. S. (2010). Business Models as Models. *Long Range Planning, 43*(2-3), 156-171. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0024630110000117

Bahl, S., Wali, O., & Kumaraguru, P. (2011). Information security practices followed in the Indian software services industry: An exploratory study. *Second Worldwide Cybersecurity Summit (WCS)*, 1-7.

Bishop, M. (2005). *Introduction to Computer Security.* Boston: Pearson Education.

Bouwman, H., De Vos, H., & Haaker, T. (2008). *Mobile Service Innovation and Business Models.* Berlin Heidelberg: Springer. doi:10.1007/978-3-540-79238-3

Cabinet Secretariat. (s.f.). *Act on the Protection of Personal Information (Act No. 57 of 2003)*. Obtenido de Cabinet Secretariat: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

Cámara Comercio Medellín. (4 de Junio de 2019). *Retos para la consolidación de las pymes en Antioquia*. Obtenido de Cámara de Comercio de Medellín para Antoquia: https://www.camaramedellin.com.co/Portals/0/Noticias/Documentos%20Noticias%202019/Presentaci%C3%B3n%20Jaime%20Echeverri.pdf?ver=2019-06-04-150220-220

Cámara de Comercio de Bogotá. (s.f.). *Clusters*. Recuperado el 2020, de CCB: https://www.ccb.org.co/Clusters

Cámara de Comercio de Medellín. (2020). *Cluster y Competitividad*. Obtenido de Cámara de Comercio de Medellín para Antioquia: https://www.camaramedellin.com.co/comunidad-cluster/que-es-la-estrategia-cluster

Canadian Centre for Cybersecurity. (2020). *Canadian Centre for Cybersecurity*. Obtenido de Baseline Cyber Security Controls for Small and Medium Organizations: https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Canadian Centre for Cybersecurity. (2021). *Baseline Cyber Security Controls for Small and Medium Organizations*. Obtenido de Canadian Centre for Cybersecurity: https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Caracol Radio. (15 de 09 de 2017). *Sector salud: el menos preocupado por resguardar los datos personales de sus clientes*. Obtenido de Caracol Radio: https://caracol.com.co/programa/2017/09/15/sanamente/1505506347_788925.html

Carey, M. J., & Jin, J. (2019). *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World* (1 ed.). USA, USA: Wiley.

Carvajal, J. E. (02 de 03 de 2021). *Paradoja de adopción tecnológica en Colombia*. Obtenido de Ude@ Educación virtual: https://udearroba.udea.edu.co/blog/paradoja-de-adopcion-tecnologica-en-colombia/

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, 135-146.

CISCO. (s.f.). *What is Information Security?* Obtenido de CISCO: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Cook, K. (2017). Effective Cyber Security Strategies for Small Businesses. *Walden University*, 1-185.

Czeschik, C. (2018). Black Market Value of Patient Data. En C. Linnhoff-Popien, R. Schneider, & M. Zaddach, *Digital Marketplaces Unleashed* (págs. XXXIII, 935). Germany: Springer-Verlag GmbH Germany.

Da Silva, G. M., Dias, G., & Lira, A. A. (2015). Proposal for Simplified Security Model for Small and Medium Business. *XI Brazilian Symposium on Information Systems*, 299-306.

Davidson, R., & Lambert, S. (2004). Applying the Australian and New Zealand Risk Management Standard to Information Systems in SMES. *Australasian Journal of Information Systems*, *12*(1), 4-17.

Davidson, R., & Lambert, S. (2004). Applying the Australian and New Zealand Risk Management Standard to Information Systems in SMES. *Australasian Journal of information Systems*, 1-14.

Dimopoulos, V., Furnell, S., Jennex, M. E., & Kritharas, L. (2004). Approaches to IT Security in Small and Medium Enterprises. *Researchgate*, 10.

Dubosson-Torbay, M., Osterwalder, A., & Pigneur, Y. (2002). E-Business Model Design,Classification, and Measurements. *Thunderbird International Business Review*,

44(1), 5-23. Obtenido de https://onlinelibrary-wiley-com.ezproxy.eafit.edu.co/doi/epdf/10.1002/tie.1036

Economía Aplicada. (2019). *¿Cuántas empresas hay en Colombia?* Obtenido de Economía Aplicada: http://economiaaplicada.co/index.php/10-noticias/1493-2019-cuantas-empresas-hay-en-colombia

eHealth Ireland. (s.f.). *eHealth Ireland*. Obtenido de Privacy: https://www.ehealthireland.ie/a2i-hids-programme/individual-health-identifier-ihi-/privacy/

eHealth Ireland. (s.f.). *Privacy*. Obtenido de eHealth Ireland: https://www.ehealthireland.ie/a2i-hids-programme/individual-health-identifier-ihi-/privacy/

El Sawy, O. A., & Pereira, F. (2013). *Business Modelling in the Dynamic Digital Space.* Los Angeles: Springer. doi: 10.1007/978-3-642-31765-1

Elteste, U., Van Quathem, K., & Oberschelp de Meneses, A. (2020). *Germany Publishes Draft Regulation on the Reimbursement of Digital Health Applications*. Obtenido de Covington Digital Health: https://www.covingtondigitalhealth.com/2020/02/german-publishes-draft-regulation-on-the-reimbursement-of-digital-health-applications/

Elteste, U., Van Quathem, K., & Shepherd, N. (2020). *German Federal Agencies Publish Privacy and IT Security Requirements for Digital Health Applications*. Obtenido de Inside Privacy: https://www.insideprivacy.com/health-privacy/germany-digav-it-security/

Eset. (18 de Junio de 2018). *Eset security Report. Latinoamerica 2018*. Obtenido de Slideshare: https://www.slideshare.net/ESETLA/eset-security-report-latinoamrica-2018

EUR-Lex. (s.f.). *Reglamento (UE) 2016/679 del parlamento europeo y del consejo.* Obtenido de EUR-Lex: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

European Commision. (s.f.). *Internal Market, Industry, Entrepreneurship and SMEs*. Obtenido de European Comission: https://ec.europa.eu/growth/smes/sme-definition_en

European Digital SME Alliance. (2019). *Skills for SMEs - Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises.* Obtenido de European Comission Executive Agency for Small and Medium-sized Enterprises (EASME) Unit A 1.3 Entrepreneurship and Clusters: https://www.digitalsme.eu/digital/uploads/Skills-for-SMEs-A-vision-and-roadmap-to-foster-adoption-of-cybersecurity-big-data-and-IoT.pdf

European Digital SME Alliance. (2020). The EU Cybersecurity Act and the role of standards for SMEs. Bruselas, Bruselas, Belgica.

Fatima, A., & Colomo-Palacios, R. (2018). Security aspects in healthcare information systems: A systematic mapping. *ScienceDirect*, 12-19.

Federal Data Protection and Information Commissioner (FDPIC). (s.f.). *II. A Few Facts about the Federal Act on Data Protection*. Obtenido de edoeb: https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/legal-framework/ii--a-few-facts-about-the-federal-act-on-data-protection.html#:~:text=The%20FADP%20provides%20an%20overall,of%20data%20by%20Federal%20authorities.

Fernández-Alemán, J., Carrión, I., Oliver, P. Á., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *ScienceDirect*, 541-562.

Fortinet. (2020). *Global Threat Landscape Report.* Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-h1-2020.pdf

Función Pública. (s.f.). *Ley 1581 de 2012.* Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20art%C3%ADculo%2015%20de%20la

Galan, C., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). *Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* Obtenido de ENISA: https://www.enisa.europa.eu/publications/standardisation-for-smes

Gand, K. (2017). Investigating on requirements for business model representations: The case of information technology in healthcare. *2017 IEEE 19th Conference on Business Informatics (CBI)*, 471-480.

Gassmann, O., Frankenberger, K., & Csik, M. (2014). *The Business Model Navigator.* Londres: Pearson.

Gomes, J., & Moqaddemerad, S. (2016). Futures Business Models for an IoT Enabled Healthcare Sector: A Causal Layered Analysis Perspective. *Journal of Business Models*, 60-80.

Gordijn, J., & Akkermans, H. (2001). e3-value: Design and Evaluation of e-Business Models. *Submission IEEE Intelligent Systems,* 17. Obtenido de https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.28.3806&rep=rep1&type=pdf

Government of Canada. (1985). *Privacy Act.* Obtenido de Justice Laws Website: https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

Government of Canada. (2000). *Personal Information Protection and Electronic Documents Act.* Obtenido de Justice Laws Website: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

Harris, S., & Maymi, F. (2016). *CISSP, All in one exam guide.* New York: McGraw-Hill Education.

Hassan, N. H., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *ScienceDirect,* 1007-1012.

Head of HSE IHI Business Service. (2017). *Individual Health Identifier Business Service Data Protection Policy.* Obtenido de ehealth Ireland: https://www.ehealthireland.ie/a2i-hids-programme/individual-health-identifier-ihi-/privacy/hse-ihi-business-service-data-protection-policy-30-may-2017.pdf

Healthcare Information and Management Systems Society. (2019). *2019 HIMSS Cybersecurity Survey.* Obtenido de HIMSS: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Healthcare Information and Management Systems Society. (2020). *2020 HIMSS Cybersecurity Survey.* Obtenido de HIMSS: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

HealthIT. (s.f.). *Health IT Legislation.* Obtenido de healthIT.gov: https://www.healthit.gov/topic/onc-hitech-programs

Hedman, J., & Kalling, T. (2003). The business model concept: theoretical underpinnings and empirical illustrations. *European Journal of Information Systems, 12*(1), 49-59.

Heikkilä, J., Tyrväinen, P., & Heikkilä, M. (2010). Designing for performance – a technique for. *Proceedings of EBRF, Research Forum to Understand Business in Knowledge Society*, 1-15.

Heikkilä, M., Bouwman, H., & Heikkilä, J. (2018). From strategic goals to business model innovation paths: an exploratory study. *Journal of Small Business and Enterprise Development*, 1-22.

Heikkilä, M., Bouwman, H., & Heikkilä, J. (2018). From strategic goals to business model innovation paths: an exploratory study. *Journal of Small Business and Enterprise Development*, 1-22.

HHS. (s.f.). *Summary of the HIPAA Security Rule.* Obtenido de Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

iapp. (2020). *Germany adopts draft patient data protection law*. Obtenido de Daily Dashboard: https://iapp.org/news/a/germany-adopts-draft-patient-privacy-law/#

iapp. (s.f.). *Regulations To The Federal Law On The Protection of Personal Data Held by Private Parties (Mexico)*. Obtenido de iapp: https://iapp.org/resources/article/regulations-to-the-federal-law-on-the-protection-of-personal-data-held-by-private-parties-mexico/

Interpol. (08 de 2020). *Un informe de Interpol muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. Obtenido de Interpol: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

ISACA. (2010). *The Business Model for Information Security.* Rolling Meadows: ISACA.

Johnson, G., Scholes, K., & Whittington, R. (2006). *Dirección estratégica.* Madrid: Pearson Educación.

Johnson, M. W., Christensen, C. M., & Kagermann, H. (2008). Reinventing Your Business Model. *Harvard Business Review*, 12.

Jones, H. (10 de 2002). *Small Firms Warned Over Hackers*. Obtenido de British Broadcasting Company, BBC News, 9: http://news.bbc.co.uk/2/hi/technology/2428983.stm

Kanta. (s.f.). *What are the Kanta Services?* Obtenido de Kanta: https://www.kanta.fi/en/what-are-kanta-services

Kaspersky. (02 de 10 de 2017). *No hay víctimas pequeñas para los cibercriminales*. Obtenido de Kaspersky: https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals

Kaspersky. (2019). *Protección continua para su negocio simple y fácil de usar*. Obtenido de Kaspersky: https://latam.kaspersky.com/small-to-medium-business-security

Kaspersky. (s.f.). *El ransomware: qué es, cómo se lo evita, cómo se elimina*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/threats/ransomware

Katz, D. R. (06 de 12 de 2017). *El observatorio de la economía digital de Colombia.* Obtenido de Cluster Bogotá Software y TI: https://bibliotecadigital.ccb.org.co/handle/11520/22589

Kissi, J., Baozhen, D., Clemency, B. A., & Amoah-Anomah, G. (2018). Reliance on Cryptography of Cloud Computing in Healthcare Information Management, Lessons for Ghana Health Service. *International Journal of Information Security Science*, 111-125.

Koyuncu, A., & Mei, V. (2020). *Germany Prepares New Law for Patient Data Protection and Increased Digitalisation in Healthcare and for "Data Donations" for Research Purposes*. Obtenido de Covington Digital Health: https://www.covingtondigitalhealth.com/2020/08/germany-prepares-new-law-for-patient-data-protection-and-increased-digitalisation-in-healthcare-and-for-data-donations-for-research-purposes/

Kriegel, J., Riedl, A., Tuttle-Weidinger, L., & Stöbich, A.-M. (2020). Future strategic topics in the business model of hospitals in Austria. *International Journal of Healthcare Management*, 101-108.

legislation.gov.uk. (2018). *Data Protection Act 2018*. Obtenido de Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Library of Congress. (s.f.). *Online Privacy Law: Netherlands*. Obtenido de Library of Congress: https://www.loc.gov/law/help/online-privacy-law/2017/netherlands.php

Lipman, P. (02 de 03 de 2020). *One In Five SMBs Don't Use Any Cybersecurity: Here's What They're Putting At Risk*. Obtenido de Forbes: https://www.forbes.com/sites/forbestechcouncil/2020/03/02/one-in-five-smbs-dont-use-any-cybersecurity-heres-what-theyre-putting-at-risk/?sh=7e736dfb7b95

Luna, D. (2017). *Primera Gran Encuesta TIC / 2017 Estudio de acceso, uso y retos de las TIC en Colombia.* Bogotá: MinTIC.

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Sci Eng Ethics*, 419-441.

Mahmood, A. (2010). *Information Security Management of Healthcare System.* Obtenido de DiVA: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A831688&dswid=2653

Malwarebytes. (s.f.). *Todo acerca del malware*. Obtenido de Malwarebytes: https://es.malwarebytes.com/malware/

Malwarebytes. (s.f.). *What is spam? Definition & types of spam*. Obtenido de Malwarebytes: https://www.malwarebytes.com/spam/

Marolleau, L. (2018). *France: France Adopts A New Data Protection Act*. Obtenido de Soulier Avocats: https://www.mondaq.com/france/data-protection/716716/france-adopts-a-new-data-protection-act

Matrane, O., & Talea, M. (2014). A Maturity Model for Information Security Management in Small and Medium-Sized. *International Journal of Advanced Research in Computer Science*, 1-6.

McCarthy, W. E. (1982). The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment. *The Accounting Review, 57*(3), 554-578. Obtenido de https://www.jstor.org/stable/246878

Miessler, D. (05 de 12 de 2018). *Information Security Concepts*. Obtenido de Daniel Miessler: https://danielmiessler.com/study/infosecconcepts/

Ministerio de Comercio, Industria y Turismo. (06 de 06 de 2019). *Decreto número 957 de 5 de junio de 2019*. Recuperado el 02 de 2020, de mincit: https://www.mincit.gov.co/getattachment/555adb9d-8a48-45f3-a2a5-1ee9b35b2d09/Decreto-957-Por-el-cual-se-adiciona-el-capitulo-13.aspx

Ministerio de comercio, industria y turismo; Departamento administativo nacional de estadística. (05 de 12 de 2019). *Resolución número 2225 de 5 de diciembre de 2019*. Obtenido de mincit: https://www.mincit.gov.co/getattachment/7e05bcde-66df-49a2-b6d2-a160f585cf54/Resolucion-2225-del-05-de-diciembre-de-2019-por-la.aspx

Ministerio de salud. (16 de 02 de 2015). *Ley estatutaria 1751 de 16 de febrero de 2015*. Obtenido de minsalud: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/INEC/IGUB/ley-1751-de-2015.pdf

Ministerio de salud. (31 de 01 de 2020). *Ley 2015 de 31 de enero de 2020*. Obtenido de minsalud: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/INEC/IGUB/ley-2015-de-2020.pdf

MinTIC. (06 de 11 de 2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME.* Obtenido de MinTIC: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Mitnick, K., & Simon, W. (2002). *The art of deception: controlling the human element of security.* USA: Wiley Publishing.

Morrisa, M., Schindehutteb, M., & Allen, J. (2005). The entrepreneur's business model: toward a unified perspective. *Journal of Business Research, 58*(6), 726-735. Obtenido de https://pdf.sciencedirectassets.com/271680/1-s2.0-S0148296300X02329/1-s2.0-S014829630300242X/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjECsaCXVzLWVhc3QtMSJIMEYCIQCFEws9K5Fp6mjI51WPaf3Cw%2F2H0LiK0jNS3gAR3JYUBwIhAKZdDxldQ%2F8A6RcUta5SSHck8uAxBG5gcRYAn9LH

MyData. (s.f). *Mydata global is an award-winning international non-profit*. Obtenido de MyData: https://mydata.org/

Nabe, C. (s.f.). *Impact of COVID-19 on Cybersecurity*. Obtenido de Deloitte: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Narayana, T., Naik, N., & Venkataiah, E. (2013). Information Security in Healthcare Sector. *International Refereed Journal of Engineering and Science (IRJES)*, 124-130.

Neveux, E. (11 de 2020). *Healthcare data: The new prize for hackers*. Obtenido de SecureLink: https://www.securelink.com/blog/healthcare-data-new-prize-hackers/#:~:text=According%20to%20a%20Trustwave%20report,record%20(a%20payment%20card).

News Center Microsoft Latinoamérica. (18 de 02 de 2021). *La transformación digital de las Pymes llegó para quedarse: 8 de cada 10 continuarán con el proceso de reinvención de su objetivo de negocio después de la pandemia*. Obtenido de News Center Latinoamérica: https://news.microsoft.com/es-xl/la-transformacion-digital-de-las-pymes-llego-para-quedarse-8-de-cada-10-continuaran-con-el-proceso-de-reinvencion-de-su-objetivo-de-negocio-despues-de-la-pandemia/#estudio

NIST. (s.f). *Accountability*. Obtenido de Computer Security Resource Center: https://csrc.nist.gov/glossary/term/accountability#:~:text=Definition(s)%3A,of%20that%20equipment%20or%20information.

NIST. (s.f.). *information security*. Obtenido de Computer Security Resource Center: https://csrc.nist.gov/glossary/term/information_security

Okundaye, K., Fan, S. K., & Dwyer, R. J. (2019). Impact of information and communication technology in Nigerian small-to medium-sized enterprises. *Journal of Economics, Finance & Administrative Science*, 29-46.

Onyango, A., Kemboi, L., & Ronoh, L. (2019). Security Control Requirements for Electronic Health Records. *International Journal of Innovative Science and Research Technology*, 1-5.

Osores, M. (09 de 02 de 2021). *Presupuesto para ciberseguridad aumenta, pese a recortes por COVID-19*. Obtenido de TechTarget: https://searchdatacenter.techtarget.com/es/noticias/252496098/Presupuesto-para-ciberseguridad-aumenta-pese-a-recortes-por-COVID-19

Osterwalder, A. (2004). *The business model ontology: A proposition in a design science approach*, 172. Lusanne: Université de Lausanne. Obtenido de http://www.hec.unil.ch/aosterwa/PhD/Osterwalder_PhD_BM_Ontology.pdf

Osterwalder, A., & Pigneur, Y. (2011). *Generación de modelos de negocio.* Barcelona: Grupo Planeta.

Osterwalder, A., Pigneur, Y., & Tucci, C. (2005). Clarifying Business Models Origins, Present, and Future of the Concept. *Communications of the Association for Information Systems, 16*(1), 28. Obtenido de https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3016&context=cais

Osterwalder, A., Pigneur, Y., Bernarda, G., & Smith, A. (2014). *Diseñando la propuesta de valor*. Barcelona: Centro libros PAPF.

Páez, G. N., Jaramillo, L. F., & Franco, C. (06 de 2013). *Estudio sobre la geografia sanitaria de Colombia*. Obtenido de Minsalud:

https://www.minsalud.gov.co/sites/rid/1/Estudio%20sobre%20la%20geograf%C3%ADa%20sanitaria%20de%20Colombia.pdf

Patterson, J. (2017). Cyber-Security Policy Decisions in Small Businesses. *Walden University*, 1-109.

Paulsen, C., & Toth, P. (2016). Small Business Information Security: The Fundamentals NISTIR 7621 Revision 1. *NIST*, 1-54.

Periódico El Sol. (2019). *La importancia de la ciberseguridad en el sector salud*. Obtenido de Elsolweb: https://elsolweb.tv/la-importancia-de-la-ciberseguridad-en-el-sector-salud/

Phishing. (s.f.). *Phishing*. Obtenido de Phishing: https://www.trendmicro.com/vinfo/us/security/definition/phishing

Picón, K. V. (17 de 07 de 2020). *La era digital y los retos del comercio electrónico en Colombia*. Obtenido de Universidad Pontificia Bolivariana: https://www.upb.edu.co/es/noticias/era-digital-retos-comercio-electronico-colombia

Policia Nacional. (30 de 03 de 2016). *Guía para evitar la suplantación de clientes y proveedores*. Obtenido de Boletín de análisis en Ciberseguridad PyME: https://caivirtual.policia.gov.co/sites/default/files/clientes_y_proveedores_0.pdf

Ponemon Institute. (03 de 2014). *Fourth Annual Benchmark Study on Patient Privacy & Data Security.* Obtenido de Ponemon Institute: https://www.ponemon.org/local/upload/file/ID%20ExpertsPatient%20Privacy%20%26%20Data%20Security%20Report%20FINAL1-1.pdf

Ponemon Institute. (05 de 2015). *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.* Obtenido de Ponemon Institute: https://iapp.org/media/pdf/resource_center/Ponemon_Privacy_Security_Healthcare_Data.pdf

Ponemon Institute LLC. (05 de 2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data.* Obtenido de Ponemon Institute: https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

Porter, M. (1996). What is strategy? *Harvard Business Review*, 61-78.

Prince, D., & King, N. (2012). *Small Business: Cyber Security Survey 2012.* Obtenido de Lancaster University: https://eprints.lancs.ac.uk/id/eprint/60274/1/sbcss2012_report.pdf

Public Health Emergency. (2017). *Health Care Industry Cybersecurity Task Force - Report on Improving Cybersecurity in the Health Care Industry*. Obtenido de Public Health Emergency: https://www.phe.gov/about/pages/default.aspx

Red Seguridad. (10 de 01 de 2020). *Impulsar la ciberseguridad, una necesidad para las pymes*. Obtenido de Red Seguridad: https://www.redseguridad.com/actualidad/impulsar-la-ciberseguridad-una-necesidad-para-las-pequenas-y-medianas-empresas_20200110.html

République Francaise. (2018). *LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1).* Obtenido de Légifrance: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952?r=RoLR1PpScV

Riigi Teataja. (2018). *Health Services Organisation Act.* Obtenido de Riigi Teataja: https://www.riigiteataja.ee/en/eli/508012018001/consolide

SANS Institute. (s.f.). *Information Security Resources*. Recuperado el 2021, de SANS: https://www.sans.org/information-security/

Schneier, B. (18 de 01 de 2007). *Information Security and Externalities*. Obtenido de Schneier on Security: https://www.schneier.com/blog/archives/2007/01/information_sec_1.html

Secretaria del Senado. (23 de 12 de 1993). *Ley 100 de 1993*. Obtenido de Secretaria del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_0100_1993.html

Secretaria Senado. (12 de 07 de 2000). *Ley 590 de 2000*. Obtenido de Secretaria Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_0590_2000.html

Secretaria Senado. (21 de 12 de 2001). *Ley 715 de 2001*. Obtenido de Secretaria del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_0715_2001.html

Secretaría Senado. (20 de Octubre de 2019). *Ley Estatutaria 1581 de 2012*. Obtenido de Secretaria del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Sectorial. (03 de 2020). *Salud*. Obtenido de Biblioteca Sectorial: https://biblioteca-sectorial-co.ezproxy.eafit.edu.co/index.php/sectores/salud

Seelos, C., & Mair, J. (2007). Profitable Business Models and Market Creation in the Context of Deep Poverty: A Strategic View. *Academy of Management Perspectives, 21*(4), 49-63.

Semana. (19 de 1 de 2007). *Tecnología, factor clave para el desarrollo de las Pyme*. Obtenido de Semana: https://www.dinero.com/columna-del-lector/opinion/articulo/tecnologia-factor-clave-para-desarrollo-pyme/40440

Semana. (12 de 8 de 2013). *Riesgos a los que se exponen las Pyme*. Obtenido de Semana: https://www.dinero.com/empresas/articulo/la-seguridad-informacion-pyme/189244

Semana. (14 de 10 de 2020). *La pandemia aceleró la transformación digital en el sector de la salud*. Obtenido de Semana: https://www.semana.com/pais/articulo/transformacion-digital-en-el-sector-de-la-salud-en-colombia/303539/

Shafer, S. M., Smith, H. J., & Linder, J. C. (2005). The power of business models. *Kelley School of Business, 48*(3), 199-207. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0007681304001132

Söderström, E., Åhlfeldt, R.-M., & Eriksson, N. (2009). Standards for information security and processes in healthcare. *Emerald Insight*, 295-308.

Sothis. (s.f.). *Cuando las amenazas son las mismas, la seguridad ha de ser la misma, independientemente del tamaño de la empresa*. Obtenido de Ciberseguridad y pyme: https://www.sothis.tech/ciberseguridad-pyme/?utm_source=red-seguridad&utm_medium=branded-content&utm_campaign=ene-20

Squire Patton Boggs. (s.f.). *Qatar's New Protection of Personal Data Privacy Law*. Obtenido de Squire Patton Boggs: https://www.squirepattonboggs.com/-/media/files/insights/publications/2017/11/qatars-new-protection-of-personal-data-privacy-law/28492--qatars-new-protection-of-personal-data-privacy-law.pdf

Stanimirovic, D. (2015). A framework for information and communication technology induced transformation of the healthcare business model in Slovenia. *Journal of Global Information Technology Management.*, 29-47.

Stanković, L., Djukić, S., & Lepojević, V. (2014). Innovation Capacities of Serbian Small and Medium-sized Enterprises. *TEME: Casopis za Društvene Nauke*, 1077-1093.

Strategizer. (s.f.). *Strategizer.* Obtenido de The Value Proposition Canvas: https://www.strategyzer.com/canvas/value-proposition-canvas

Strategizer. (s.f.). *Strategizer*. Obtenido de The Business Model Canvas: https://www.strategyzer.com/canvas/business-model-canvas

Subramoniam, S., & Sadi, S. (2010). Healthcare 2.0. *IT Professional IT Prof. IT Professional.* , 46-51.

Supersalud. (06 de 2019). *Informe resultados financieros del sector salud. Núm 4*. Obtenido de Supersalud: https://docs.supersalud.gov.co/PortalWeb/metodologias/Informes%20de%20Estudios%20Sectoriales/Resultados%20Financieros%20SGSSS%202018.pdf

Supersalud. (07 de 2020). *Informe Resultados Financieros del Sector Salud. Núm 5.* Obtenido de Supersalud: https://docs.supersalud.gov.co/PortalWeb/metodologias/Informes%20de%20Estudios%20Sectoriales/Resultados%20Financieros%20SGSSS%202019.pdf

The Federal Servie for Supervision of Communications, Information Technology. (s.f.). *Roskomnadzor*. Obtenido de Federal Law of 27 July 2006 N 152-FZ ON PERSONAL DATA: https://pd.rkn.gov.ru/authority/p146/p164/

The Privacy Protection Authority. (2017). *Protection of privacy regulations (data security) 5777-2017*. Obtenido de gov.il: https://www.gov.il/en/Departments/legalInfo/data_security_regulation

The Privacy Protection Authority. (2021). *Privacy Protection (Data Security) Regulations.* Obtenido de gov.il: https://www.gov.il/en/departments/general/data_security_eng

The Swedish Data Protection Authority. (s.f.). *The Swedish Data Protection Authority*. Obtenido de itgovernance.eu: https://www.itgovernance.eu/sv-se/eu-gdpr-compliance-se

Tian, C. H., Ray, B. K., Lee, J., Cao, R., & Ding, W. (2008). BEAM: A framework for business ecosystem analysis and modeling. *IBM Systems Journal, 47*(1), 101-114. doi:10.1147/sj.471.0101

Timmers, P. (1998). Business Models for Electronic Markets. *Electronic Markets, 8*(2), 3-8. doi:10.1080/10196789800000016

Trustwave. (2018). *Trustwave Global Security Report.* Obtenido de Trustwave: https://www.shift4.com/pdf/Trustwave_2018_Global_Security_Report.pdf

U.S. Small Business Administration. (s.f). *Opciones de asistencia por COVID-19*. Obtenido de SBA: https://www.sba.gov/

Vector ITC. (21 de 05 de 2018). *El desconocimiento es la mayor amenaza a la ciberseguridad.* Obtenido de Vector ITC a softtek Company: https://www.vectoritcgroup.com/tech-magazine/cybersecurity/el-desconocimiento-es-la-mayor-amenaza-a-la-ciberseguridad/

Von Roessing, R. (2010). The ISACA Business Model for Information Security: An Integrative and Innovative Approach. *Isse 2009 Securing Electronic Business Processes*, 48-58.

Weill, P., & Vitale, M. (2001). *Place to Space: Migrating to eBusiness Models.* Harvard Business School Publishing Corporation.

WHO. (2019). *World Health Statistics 2019.* Obtenido de World Health Organization: https://apps.who.int/iris/bitstream/handle/10665/324835/9789241565707-eng.pdf?ua=1

Williams, N. (2013). A Strategic Model for Information Security Growth in Small and Medium Enterprises. *Researchgate*, 1487-1495.

Yang, Y. (2018). Literature Review of Information Security Practice Survey Reports. *Jyväskylä: University of Jyväskylä*, 1-95.

Yaping, Y. (2018). *Literature Review of Information Security Practice Survey Reports.* Obtenido de Literature Review of Information Security Practice Survey Reports: https://jyx.jyu.fi/bitstream/handle/123456789/59443/1/URN%3ANBN%3Afi%3Ajyu-201809064034.pdf